A Novel IGDT-Based Method to Find the Most Susceptible Points of Cyberattack Impacting Operating Costs of VSC-Based Microgrids

Davari, Masoud; Nafisi, Hamed; Nasr, Mohamad-Amin; Blaabjerg, Frede

Published in:
I E E E Journal of Emerging and Selected Topics in Power Electronics

DOI (link to publication from Publisher):
10.1109/JESTPE.2020.3015447

Publication date:
2021

Document Version
Accepted author manuscript, peer reviewed version

Citation for published version (APA):
Davari, M., Nafisi, H., Nasr, M-A., & Blaabjerg, F. (2021). A Novel IGDT-Based Method to Find the Most Susceptible Points of Cyberattack Impacting Operating Costs of VSC-Based Microgrids. *I E E E Journal of Emerging and Selected Topics in Power Electronics*, *9*(3), 3695 - 3714. [9163351]. https://doi.org/10.1109/JESTPE.2020.3015447

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JESTPE.2020.3015447, IEEE Journal of Emerging and Selected Topics in Power Electronics

A Novel IGDT-Based Method to Find the Most Susceptible Points of Cyberattack Impacting Operating Costs of VSC-Based Microgrids

Masoud Davari*, *Senior Member, IEEE*, Hamed Nafisi, Mohamad-Amin Nasr, and Frede Blaabjerg, *Fellow, IEEE*

***Abstract*—This paper proposes a novel mathematical approach to deal with cyberattacks impacting on modernized microgrid's tertiary control. Modernized microgrids use many entities based on voltage-source converters to form the fully integrated power and energy system. Having such a power and energy system for modernized microgrids necessitates engineers considering cybersecurity and addressing its effects from the beginning of designing and building systems. Using innovative mathematical tools based on information gap decision theory (also known as IGDT), this paper incorporates the data integrity attacks into tertiary controls of the fully integrated power and energy system of modernized microgrids. The proposed methodology [named cyberattack-tolerant tertiary control (CT^{2}C) herein] is able to effectively find the most susceptible points of cyberattack in modernized microgrids when both severe and negligible uncertainties caused by cyberattacks take place. They are able to include both severe data integrity attacks and negligible ones (or undetectable attacks). Here, the most vulnerable points of cyberattack cause the most impactful changes in the tertiary control's principal objective, which is minimizing the operating cost of the whole modernized microgrids. In this regard, this paper describes a hypothesis, and in supporting that, comparative simulation results are given. The outcomes generated by the General Algebraic Modeling System (commonly known as GAMS) environment are able to provide researchers and engineers with appropriate maps for sensitive points of cyberattack. Using the proposed CT^{2}C, investments in modernized microgrids cybersecurity will be more accurate and, more importantly, mathematically optimized. Finally, potential ways to implement the proposed methodology are elaborated.**

***Index Terms*—Cyberattack (CA), fully integrated power and energy system (FIPES), information gap decision theory (IGDT), modernized microgrid (MMG), operating cost (OC), points of cyberattack (PoCA), tertiary control.**

This work was supported by the U.S. National Science Foundation (NSF) under Grant #1808279 and Grant #1902787 provided by the Core Program of Energy, Power, Control, and Networks (EPCN) in the Division of Electrical, Communications and Cyber Systems (ECCS), and it has been tested entirely at Georgia Southern University (Statesboro Campus).

Masoud Davari is with the Department of Electrical and Computer Engineering, Allen E. Paulson College of Engineering and Computing, Georgia Southern University (Statesboro Campus), Statesboro GA 30460, USA, e-mails: mdavari@georgiasouthern.edu *and* davari@ualberta.ca.

Hamed Nafisi and Mohamad-Amin Nasr are with the Center of Excellence in Power Systems, Department of Electrical Engineering, Amirkabir University of Technology, Tehran 15914, Iran (e-mails: nafisi@aut.ac.ir and m.amin.nasr@aut.ac.ir).

Frede Blaabjerg is with the Department of Energy Technology, Aalborg University, Aalborg, Denmark DK-9220, e-mail: fbl@et.aau.dk.

**Corresponding Author*.

NOMENCLATURE

Subscripts and superscripts

g	Generating unit
i, j	Bus
l	Line between the i^{th} and j^{th} buses
n	Battery energy storage system unit
z	Uncertain parameter

Variables

δ_{CA}	Tolerable increment in operating cost considering the vulnerability of tertiary controls to cyberattacks [pu]
δ_{i,k_t}	Voltage angle [radian]
κ_z	Uncertainty horizon
κ_{z,k_t}	Uncertainty horizons at each time interval in the information gap decision theory (IGDT)-based tertiary control
λ_{g,k_t}	Shutdown decision ("1" = shutdown and "0" = otherwise)
μ_{g,k_t}	Start-up decision ("1" = start-up and "0" = otherwise)
Π	System input/output structure
Θ_{g,k_t}	On/off decision ("1" = on and "0" = off)
$\tilde{R}_z$	Robustness band of z^{th} uncertain parameter
$I^{\text{ch}}_{n,k_t}/I^{\text{dch}}_{n,k_t}$	Charging/discharging decision ("1" = allowed and "0" = not allowed)
OC	Operating cost [$]
P_{g,k_t}, Q_{g,k_t}	Active/reactive power of generating units [pu]
P_{loss,k_t}	Total active power loss [pu]
$P^{\text{dch}}_{n,k_t}/P^{\text{ch}}_{n,k_t}$	Battery energy storage system discharging/charging power [pu]
RoU	Radius of uncertainty defined by variables K_{DG}, K_{BESS}, K_{PV}, K_{WT}, and K_{Load} for different entities [pu]
S_{i,j,k_t}	Apparent power transfer [pu]
$T^{\text{off}}_{g,k_t}/T^{\text{on}}_{g,k_t}$	Down/up time of generating units [h]
V_{i,k_t}	Bus voltage [pu]

Parameters

Δt_{k_t}	Absolute time between interval k_t and k_{t+1} [h]
$\eta^{\text{ch}}_n/\eta^{\text{dch}}_n$	Charging/discharging efficiencies of battery energy storage systems
$\theta_{i,j}$	Angle of elements in Y_{bus} [radian]
$\tilde{\varphi}_{z,k_t}$	Predicted value of uncertain parameters
φ_{z,k_t}	Value of uncertain parameters
a_g	Quadratic term of cost function [$/(kWh)^2]

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JESTPE.2020.3015447, IEEE Journal of Emerging and Selected Topics in Power Electronics

b_g	Linear term of cost function [$/kWh]
$C_g^{\text{sdn}}/C_g^{\text{sup}}$	Shut-down/start-up cost of generating units [$]
c_g	Constant term of cost function [$/h]
G_l	Conductance of l^{th} branch
$P_{BESS_n}^{\max}$	Maximum active power of battery energy storage systems
$P_g^{\max}/P_g^{\min}$	Maximum/minimum active power of generating units [pu]
$PD_{i,k_t}/QD_{i,k_t}$	Active/reactive power demand [pu]
PV_{i,k_t}	Active power of photovoltaic units [pu]
$PW_{i,k_t}/QW_{i,k_t}$	Active/reactive power of wind turbines [pu]
$Q_g^{\max}/Q_g^{\min}$	Maximum/minimum reactive power of generating units [pu]
R_g^{dn}	Ramp down rate of generating units [pu/h]
R_g^{up}	Ramp up rate of generating units [pu/h]
RES_{k_t}	Spinning reserve requirement [pu]
S_{base}	Base apparent power [kVA]
SOC_{n,k_t}	State of charge of battery energy storage systems [pu]
$SOC_n^{\max}$	Maximum state of charge of battery energy storage systems [pu]
$SOC_n^{\min}$	Minimum state of charge of battery energy storage systems [pu]
$T_g^{\text{dn}}/T_g^{\text{up}}$	Minimum down/up time of generating units [h]
$Y_{i,j}$	Absolute value of elements in Y_{bus} [pu]
Sets	
χ_{k_t}	Decision variables in the IGDT principles
$\mathcal{B}$	System buses
$\mathcal{E}$	Battery energy storage systems
$\mathcal{G}/\mathcal{G}_i$	All diesel gensets/diesel gensets connected to the i^{th} bus
$\mathcal{L}$	System lines
$\mathcal{T}$	Time intervals
$\mathcal{Z}$	Uncertain parameters
Π_{min}	Minimum system requirements in the IGDT principles
ψ_{z,k_t}	Possible values of uncertain parameters in the IGDT principles

I. INTRODUCTION

ALTHOUGH the power networks have been utilized by "micro" grids using *localized generation and a limited distribution network*—which dates back to the beginning of the power industry—the usage of new microgrids in the traditional interconnected power systems has again started since 2002 [1]. Although those microgrids have been making use of communications and controls, they have been less dependent on advanced communication systems and sophisticated controls (similar to conventional power systems). Once smart grids have started come into existence, the traditional microgrids regard as a great assess to those power networks' operation and controls. One of the essential elements in smart grids is having more advanced, revolutionary, modern controls, along with communications, as per the Energy Independence and Security Act of 2007 (EISA-2007), which was approved by the U.S. Congress in January 2007 and signed into law in December 2007 [2].

Furthermore, the energy sector has made remarkable progress in integrating energy storage systems (e.g., battery systems) into current power networks forming ac/dc grids significantly. They may create either multi-infeed ac/dc power systems (e.g., in transmission systems) or hybrid ac/dc microgrids (e.g., in distribution systems)—under the umbrella of smart grids [3]–[12]. Once traditional hybrid ac/dc microgrids are highly employed in serving modernized smart grids, they need to have advanced controls. Those microgrids have been named "modernized microgrids" (MMG) in this research as they are equipped with sophisticated controls and communications. In smart grids, the MMG concept adds many benefits to the operation, control, and demand supply within commercial power systems.

The utilization of battery energy storage systems (BESSs) in microgrids was proposed when their paradigm was introduced [1]. MMGs will benefit from the usage of BESSs, which are presently mature enough to be applied in the bulk electric power generation and electrical energy storage. Bulk generation of BESSs (in the power industry) has recently been feasible—as BESS's technology is now mature enough to be used in pilot microgrid projects [8], [10], [13]—compared to its achievability in 2002.

MMGs take advantage of a lot of entities using power electronic converters, mainly in the form of voltage-source converters (VSCs) [12], [14]. It is noteworthy that this research considers VSCs since the other types of power electronic converters [e.g., forced-commutated current-source converters (CSCs)] have not been as widely used for applications in power systems. CSCs have not been as widely used for applications in power systems as they require controllable bipolar electronic switches, whose widespread commercial supply is not fully established by the power semiconductor industry yet. Although bipolar versions of the Gate-Turn-Off Thyristor (commonly known as GTO) and the Integrated Gate-Commutated Thyristor (also known as IGCT) are commercially available, they have limitations on switching speed, thus being primarily utilized in very high-power electronic converters. Also, for the power range of microgrids (and also MMGs), the VSCs are the dominant technology in the power electronics industry [14]. The VSCs to which this paper refers should interface different subsystems. That is why they have been referred to as the general term of "VSC"s since their mode of operation is not required to be specified as per the scope of this research. In other words, VSCs may interface a dc subsystem to an ac subsystem—with either a unidirectional power flow [7], [15] or a bidirectional one [12]—depending on the required power flow. A converter is called a rectifier if the flow of average power is from the ac side to the dc side, while it is called an inverter if the average power flow is from the dc side to the ac side. A similar statement can be discussed for the buck, boost, buck/boost, and more. As a result, the term VSC is kept without loss of generality in this work [14].

A future VSC-based MMG will employ a new trend in its power structure, called a fully integrated power and energy

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JESTPE.2020.3015447, IEEE Journal of Emerging and Selected Topics in Power Electronics

system (FIPES)—thanks to the integration of BESSs—as discussed in this paper. Fig. 1 shows a concept of a VSC-based MMG (hereinafter, referred to as MMG for ease of reference) with an FIPES. FIPESs have a similar structure to what is employed in traditional power systems, but they substantially integrate energy storage units. Those units are mostly in the form of BESSs based on the presently mature, industrial energy storage technologies. MMGs' FIPES should be given special consideration for their studies and analyses because the technologies related to storing electrical energy have been rapidly evolving in the power industry. As such, they bring more flexibility and contribute to the performances of MMGs. FIPESs are able to integrate energy systems into power systems to feed the needs of MMGs for operation, energy management, electricity market (e.g., energy arbitrage), power quality requirements, dynamics, and control.

As regards the hierarchical controls of all microgrids, they have various time intervals and horizons—ranging from milliseconds (i.e., inner control loop, as well as the primary controls), milliseconds to seconds (i.e., secondary controls), and seconds to minutes (i.e., tertiary controls). Briefly speaking, they are detailed as follows. Inner control loops, as well as the primary controls, are regulating the voltage and frequency to their reference values. The secondary control is adjusting the deviations in both voltage and frequency. The tertiary control manages the power flow of the microgrid via controlling voltage amplitude/phase of buses. Tertiary control is the highest (and hence the slowest) control level that considers economic concerns in the optimal operation of the microgrid—at the sampling time of T_s ranging from minutes to hours—and manages the optimal power flow and energy between the microgrid and the main power network. Therefore, it considers the microgrids' operating costs, as well as their efficiency economically. This paper has focused on the tertiary controls utilizing advanced communication infrastructures, which enable "modernized microgrids" to function optimally for power flow. Such structures will be supervised by a central control and an *energy management system* at the highest level, also known as the "tertiary control." In MMGs, the tertiary control is able to benefit from distributed dispatching, which allows online actions for every load change in real-time, in direct contrast to longer time scales with static demand input in the centralized schemes. It achieves more flexibility in control under issues such as transmission delay, information failure, and so on, thus improving the economic profile for optimal utilization of resources. Nevertheless, it has cyber layer imperfections (see [16] and references therein.)

Cyber threats nowadays require designers to consider cybersecurity and remove (or attenuate) its effects from the outset of designing and building engineering systems. This research will fundamentally investigate this requirement for the challenging application of tertiary controls using presently practical, industrial, networked controls. Several studies and industrial works have considered power grid cybersecurity issues, concerns, and solutions [17]–[24]. Additionally, many works on microgrid operations and controls focus on the economic aspects of microgrids (see [25]–[27] and references therein).

For instance, the authors of [16] have studied two cost-prioritized droop schemes for distributed generators in a rural or islanded microgrid. In [28], the authors have proposed a multi-agent energy storage system aggregation as a tool for scaling energy management to low voltage microgrids with distributed energy storage systems using the microgrid's tertiary controls. In [29], the researchers have proposed a voltage-frequency management technique that retains those quantities within acceptable limits in remote islanded microgrids and is activated when existing techniques for controlling energy storage systems or adjusting the set-points of generators are unsuccessful. Researchers in [30] have also suggested a reinforcement-learning-based online optimal control method for the hybrid energy storage system in ac/dc microgrids. Finally, the authors of [5] have researched scheduling generators in a day-ahead power system operation through a security-constrained unit commitment model; in order to solve this model, they have introduced a data-driven stochastic optimization that incorporates the superiority of both stochastic and robust approaches.

Additionally, some researchers have recently researched some novel aspects of the cybersecurity issues in smart grids [31]–[35]. Although secure *smart world* based on internet of things have wholly been discussed in [31] (and references therein)—which is a survey article—the potentially "unnoticeable" cyberattacks' (CAs') impacts on the tertiary controls of microgrids under the umbrella of smart grids have been overlooked. The authors in [32], [33] have discussed false data injection into the state estimation problem of smart grids, so the problem under study has not ever considered how CAs are able to increase generation costs unnoticeably. Among a lot of research on the topic mentioned earlier, [34] has investigated optimal power flow (OPF) in smart grids, but it is not fully applicable to an MMG with the FIPE as detailed in the next paragraph. Also, the authors in [35] have studied economic dispatch in a smart grid, but it has some serious shortcomings to be able to be employed in MMGs having FIPESs—as delineated in the second following paragraph.

As described in [6], [34], CAs affect the optimal energy management done in tertiary controls. However, the researchers in [6], [34] have stated that none of the latest research studies have thoroughly taken into account the CAs' influence on the "unnoticeable" increase in generation costs in the energy management system—optimally and mathematically. Indeed, none have considered a mathematical way to determine the effects of CAs; notably, the data integrity attack by CAs is the main focus here because this type of CA is not easily recognizable. It is a CA that can significantly affect the tertiary control by modifying data and manipulating it over a long time. Unauthorized insertion, deletion, and modification are among the ways causing data integrity attacks. Such CAs can cause considerable economic effects on many types of systems (e.g., see [36]) and especially the MMGs' operation discussed in this article. Even though the writers of [34] have studied data integrity attacks against OPF in smart grids, they have not considered energy management constraints; they have only taken into account the power equations. It is impossible to apply their approach to MMGs (which have FIPESs and are

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JESTPE.2020.3015447, IEEE Journal of Emerging and Selected Topics in Power Electronics

able to *store* electrical energy) because the constraints related to *storing* electrical energy cannot be considered (and should not have been seen) in the OPF problem proposed in [34]. This limitation is because of dealing with a "power" system in [34]—not a "power and energy" system.

Furthermore, [35] has mathematically researched distributed economic dispatch problem under attacks as well. Albeit [35] provides a substantial mathematical background of the problem, it has the following deficiencies. 1) Only fossil-fuel-based generations have been considered, so renewables have been overlooked. 2) Only ac grids have been seen. 3) Generating units based on energy-storing systems (e.g., BESSs) have entirely been ignored. 4) Decision-making integer variables (e.g., on/off) have been disregarded. 5) Last but not least, the impact of CAs on the generation costs have not been formulated and mathematically shown. Regarding the fifth point mentioned earlier, [35] is not able to provide a clear understanding of how much CAs are able to influence generation costs. Additionally, the proposed problem does not apply to the FIPESs of MMGs, which have a lot of new entities communicating with the central controls. Researchers may have well maturely researched the state estimation problem's vulnerabilities to the disturbances made by data integrity attacks, data false injection attacks, and so on in smart grids (e.g., [31]–[35]) and traffic control systems (e.g., [37]). Nonetheless, up to the authors' best knowledge, there is no solid research in *data integrity attacks*' effects on the increase in generation costs—or equivalently decrease in electrical energy efficiency—from the standpoint of both power engineering and mathematics.

Consequently, the power industry requires new analytical approaches to provide sufficiently accurate, qualitative information on how CAs and cybersecurity affect tertiary controls. This mathematical tool will make MMG's cybersecurity-related efforts more efficient and, more importantly, economically optimal. In this regard, new approaches need to be developed to indicate zones in MMGs that are more susceptible to CAs using appropriate mathematical tools, thus incorporating the impact of CAs into the tertiary controls of FIPES. In this direction, this article proposes a methodology and develop an algorithm to incorporate CAs into tertiary controls using an innovative optimization problem that considers the maximum available power both with and without CAs for distributed energy resources (e.g., wind, solar, battery energy storage systems, etc.) and loads.

For the tertiary control of the FIPES of MMGs, an optimization algorithm is always involved and being developed. It should be able to identify the most susceptible points of cyberattack (PoCA) associated with the data integrity attacks in order to achieve more resilient modernized grids. Some limits must unquestionably be taken into account. In other words, the more susceptible entities (including ac/dc generation, BESSs, and consumption) that impact the performance of the tertiary control once a CA occurs must be determined. In this regard, it is required to ensure that the objective function associated with the operating costs is still able to give an "optimal" solution when considering CAs.

Note that this paper investigates CAs that are not destructive to MMGs. In other words, CAs that do not take harmful actions (such as opening a breaker, etc.) and that solely inject data integrity attack into the tertiary controls; Fig. 2 shows typical CAs affecting MMG's tertiary controls. This work also regards the aforementioned data integrity attack by CAs as both "severe uncertainty" and "negligible uncertainty" of the variable under study with a "random" radius of uncertainty (RoU). Random RoUs are able to take into account both severe data integrity attacks and negligible ones (or undetectable attacks). For doing so, this article considers that RoU in the optimization process using the model proposed here. The first main objective of this research is to formulate the impacts of data integrity attacks on the tertiary controls of MMGs. They have an FIPES structure with various feasible ac/dc entities and generating units. The second one is to calculate different RoUs to find the most vulnerable PoCAs mathematically. One should consider that the latter objective is required to make conservative investments in the cybersecurity for removing (or diminishing) data integrity attack's effects on operating costs. It results in a better understanding of the CAs' impacts on tertiary controls. This way, investments enhancing cybersecurity in the MMGs' FIPES will be made rational, scientific, and more quantitative.

This paper's results are able to analytically (and illustratively) inform design engineers of the impacts of the investments in the MMGs' cybersecurity so that they are assured that data integrity attacks do not endanger the economic optimization through examining the effects of their investment. In other words, the amount of increase in operating costs is mathematically found and visually demonstrated. Therefore, that cost increase will be one of the analytical bases for the cybersecurity investment associated with MMGs. As regards this matter, [38] explicitly reports, "*The challenge for regulators lies in determining whether a particular investment is prudent, or whether other needed investments are being overlooked. Unfortunately, many regulators lack the expertise to make these judgments. In addition, the task is complicated by the "public goods" nature of many cybersecurity investments. To the extent that the benefits of a given investment (or conversely, the costs of a failing to make the investment) extend beyond an individual company, that company can be expected to underinvest from the perspective of the system as a whole. Moreover, current regulatory processes tend to overlook systemic risks*." Also, [39] clearly commented, "*Some utilities have also asked for oversight in the upgrading of utility cyber security systems and the updating of cyber insurance policies. In particular, DOE could work directly with utilities and industry suppliers to assess cyber security investments by developing metrics for evaluation of these investments. Additionally, DOE or other government agencies could provide funding to cyber security research efforts in industry, with a specific focus on evaluating new investments in cyber security and the relative effectiveness of these investments in protecting utilities against cyber attacks.*"

The contributions of this paper are as follows.

1) It derives a tertiary control for the "daily energy" management for 24 hours of the day—not solely power management—which: i) minimizes the use of diesel

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JESTPE.2020.3015447, IEEE Journal of Emerging and Selected Topics in Power Electronics

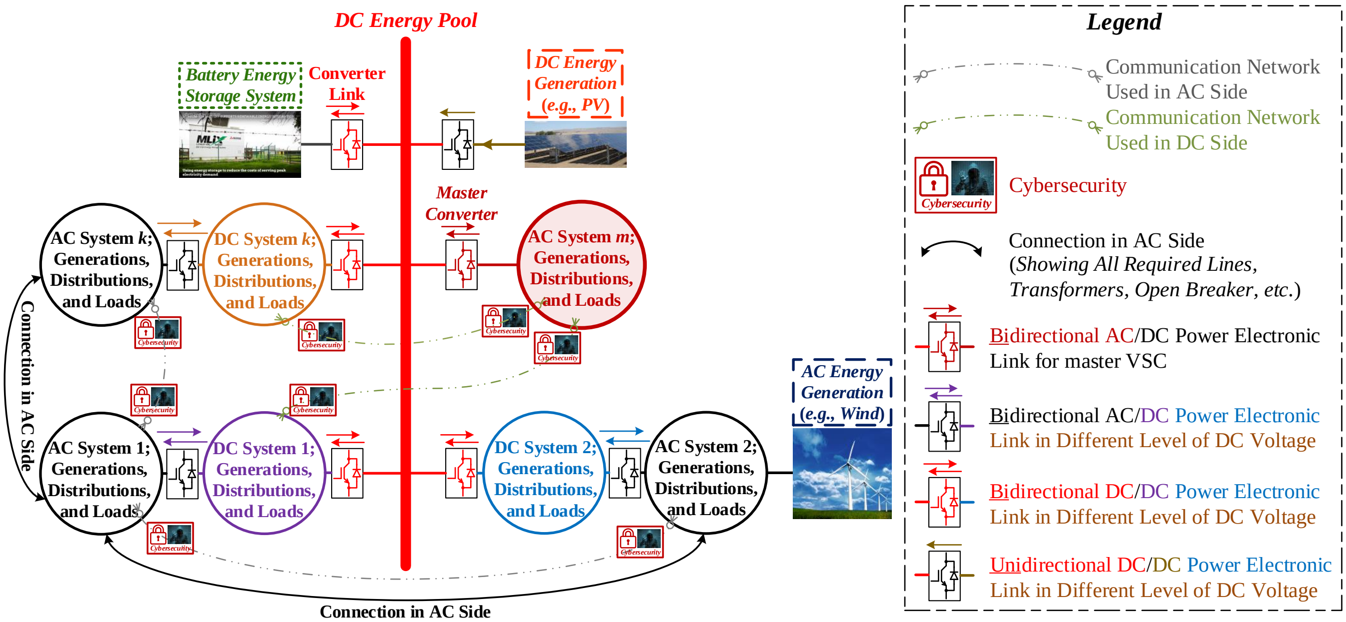

Fig. 1. Concept of the MMG's FIPES.

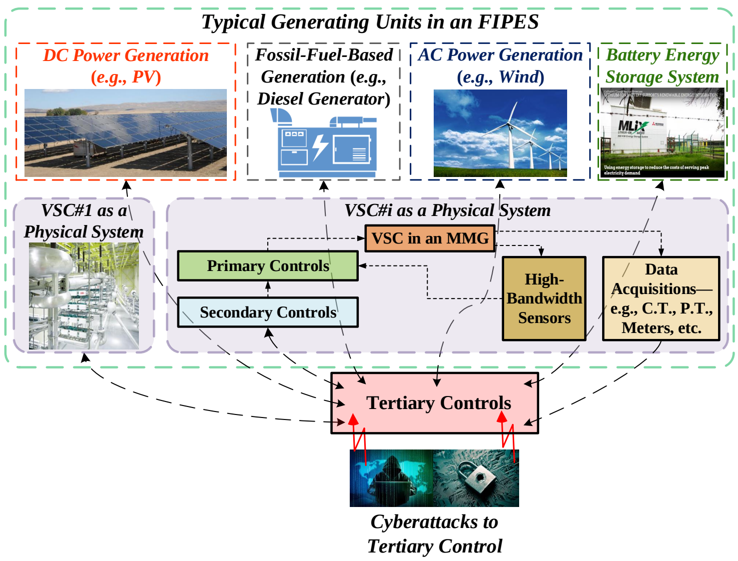

Fig. 2. Cyberattacks impacting the controls of the FIPES of an MMG—also showing a broad overview of the areas and points that may potentially be "cyberattacked" (e.g., by data integrity attacks) in the tertiary control.

generators; ii) reduces the amount of exchanged power between the ac and dc grids of the MMG; iii) drives the battery banks to be fully charged; iv) forces the battery banks to supply any power shortage with high priority; and v) satisfies power demand with maximum utilization of renewable resources.

2) It mathematically models data integrity attacks into the optimization algorithm of the tertiary control of the FIPES of MMGs. In other words, it mathematically considers the unnoticeable increase in generation costs in the FIPES's energy management system of MMGs.
3) It particularly applies applies information gap decision theory (IGDT)—as an appropriately selected mathematical tool—to the proposed problem formulation. IGDT helps decision makers manage uncertain systems without the availability of statistical data of the unknown parameters.

The remainder of this paper is structured as follows. Section II discusses the detailed tertiary control that is required to be considered in the FIPES of MMGs. Section III elaborates on the hypothesis, the proposed problem formulation, and the proposed IGDT-based methodology—named cyberattack-tolerant tertiary control (CT^{2}C)—in the FIPES. It details the proposed approach to both severe and negligible data integrity attacks. Section IV describes the case studies and discusses the simulation results for both severe and insignificant data integrity attacks. Finally, Section IV draws conclusions based on the findings from this research.

II. Detailed Tertiary Control in the FIPES

This section mathematically describes the detailed tertiary controls of the FIPES of an MMG. It takes into account all

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JESTPE.2020.3015447, IEEE Journal of Emerging and Selected Topics in Power Electronics

possible constraints to be included in the objective function of the MMG's tertiary controls. In this regard, the following equations are able to represent the generally applied operating cost (OC) for the tertiary control of FIPES of MMGs—including total generation cost, active/reactive power balance, and active power losses. It is worthy of mention that the tertiary control taken into account here is genuinely comprehensive and detailed. In this regard, this paper considers the followings: 1) active/reactive power balance, 2) active power losses, 3) lower/upper bounds of the generating units, 4) ramp up/down rates of the generating units, 4) the state of charge (SOC) of BESSs, 5) the charging/discharging power of BESSs, 6) reserve capacity, and so on. These are also considered in the unit commitment-optimal power flow [5]. The problem mentioned above formulation can also be rewritten as follows. Indeed, the following equation describes the operating cost for the tertiary control of FIPES of MMGs—*Subject To* the constraints expressed via (2)–(20).

$$\text{Minimize}\, OC = \sum_{k_t \in \mathcal{T}} \sum_{g \in \mathcal{G}} [\{(a_g (S_{base} P_{g,k_t})^2 + b_g S_{base} P_{g,k_t}) + c_g \Theta_{g,k_t}\} \Delta t_{k_t} + C_g^{\text{sup}} \mu_{g,k_t} + C_g^{\text{sdn}} \lambda_{g,k_t}], \quad (1)$$

Subject To:
Active Power Balance Equation:

$$\sum_{g \in \mathcal{G}_i} (P_{g,k_t} \Theta_{g,k_t}) + PW_{i,k_t} + PV_{i,k_t} - PD_{i,k_t} + \sum_{n \in \mathcal{E}} (P_{n,k_t}^{\text{dch}} - P_{n,k_t}^{\text{ch}}) = \sum_{j \in \mathcal{B}} V_{i,k_t} V_{j,k_t} Y_{i,j} \cos(\theta_{i,j} + \delta_{j,k_t} - \delta_{i,k_t}), \quad \forall i,j \in \mathcal{B}, \forall k_t \in \mathcal{T}, \quad (2)$$

Power Loss Equation:

$$P_{loss,k_t} = \sum_{l \in \mathcal{L}} G_l (V_{i,k_t}^2 + V_{j,k_t}^2 - 2 V_{i,k_t} V_{j,k_t} \cos(\delta_{i,k_t} - \delta_{j,k_t})), \quad \forall i,j \in \mathcal{B}, \forall k_t \in \mathcal{T}, \quad (3)$$

Reactive Power Balance Equation (Only in the AC Side):

$$\sum_{g \in \mathcal{G}_i} (Q_{g,k_t} \Theta_{g,k_t}) + QW_{i,k_t} - QD_{i,k_t} = - \sum_{j \in \mathcal{B}} V_{i,k_t} V_{j,k_t} V_{i,j} \sin(\theta_{i,j} + \delta_{i,k_t} - \delta_{i,k_t}), \quad \forall i,j \in \mathcal{B}, \forall k_t \in \mathcal{T}, \quad (4)$$

Lower and Upper Bounds of Active Power of Generating Units:

$$P_g^{\text{min}} \Theta_{g,k_t} \le P_{g,k_t} \le P_g^{\text{max}} \Theta_{g,k_t}, \ \forall g \in \mathcal{G}, \forall k_t \in \mathcal{T}, \quad (5)$$

Lower and Upper Bounds of Reactive Power of Generating Units (Only in the AC Side):

$$Q_g^{\text{min}} \Theta_{g,k_t} \le Q_{g,k_t} \le Q_g^{\text{max}} \Theta_{g,k_t}, \ \forall g \in \mathcal{G}, \forall k_t \in \mathcal{T}, \quad (6)$$

Ramp-up Rate of Generating Units:

$$P_{g,k_t+\Delta t_{k_t}} - P_{g,k_t} \le R_g^{\text{up}} \Delta t_{k_t} + \mu_{g,k_t+\Delta t_{k_t}} P_g^{\text{min}}, \quad \forall g \in \mathcal{G}, \forall k_t \in \mathcal{T}, \quad (7)$$

Ramp-down Rate of Generating Units:

$$P_{g,k_t} - P_{g,k_t+\Delta t_{k_t}} \le R_g^{\text{dn}} \Delta t_{k_t} + \lambda_{g,k_t+\Delta t_{k_t}} P_g^{\text{min}}, \quad \forall g \in \mathcal{G}, \forall k_t \in \mathcal{T}, \quad (8)$$

Minimum Up-Time Constraint:

$$[T_{g,k_t-\Delta t_{k_t}}^{\text{on}} - T_g^{\text{up}}][\Theta_{g,k_t} - \Theta_{g,k_t-\Delta t_{k_t}}] \ge 0, \quad \forall g \in \mathcal{G}, \forall k_t \in \mathcal{T}, \quad (9)$$

Minimum Down-Time Constraint:

$$[T_{g,k_t-\Delta t_{k_t}}^{\text{off}} - T_g^{\text{dn}}][\Theta_{g,k_t-\Delta t_{k_t}} - \Theta_{g,k_t}] \ge 0, \quad \forall g \in \mathcal{G}, \forall k_t \in \mathcal{T}, \quad (10)$$

Start-up and Shut-down Decisions:

$$\mu_{g,k_t} - \lambda_{g,k_t} = \Theta_{g,k_t} - \Theta_{g,k_t-\Delta t_{k_t}}, \ \forall g \in \mathcal{G}, \forall k_t \in \mathcal{T}, \quad (11)$$

*Constraint on Not Turning On **and** Off A Generating Unit Simultaneously:*

$$\mu_{g,k_t} + \lambda_{g,k_t} \le 1, \ \forall g \in \mathcal{G}, \forall k_t \in \mathcal{T}, \quad (12)$$

BESS's SOC's Equation Using Charging/Discharging Power and Efficiency:

$$SOC_{n,k_t+\Delta t_{k_t}} - SOC_{n,k_t} = [P_{n,k_t}^{\text{ch}} \eta_n^{\text{ch}} - \frac{P_{n,k_t}^{\text{dch}}}{\eta_n^{\text{dch}}}] \Delta t, \quad \forall n \in \mathcal{E}, \forall k_t \in \mathcal{T}, \quad (13)$$

SOC Lower and Upper Bounds of the BESSs:

$$SOC_n^{\text{min}} \le SOC_{n,k_t} \le SOC_n^{\text{max}}, \ \forall n \in \mathcal{E}, \forall k_t \in \mathcal{T}, \quad (14)$$

BESS's Maximum Charging Power:

$$0 \le P_{n,k_t}^{\text{ch}} \le P_{BESS_n}^{\text{max}} I_{n,k_t}^{\text{ch}}, \ \forall n \in \mathcal{E}, \forall k_t \in \mathcal{T}, \quad (15)$$

BESS's Maximum Discharging Power:

$$0 \le P_{n,k_t}^{\text{dch}} \le P_{BESS_n}^{\text{max}} I_{n,k_t}^{\text{dch}}, \ \forall n \in \mathcal{E}, \forall k_t \in \mathcal{T}, \quad (16)$$

*Constraint on Not Charging **and** Discharging A BESS Simultaneously:*

$$I_{n,k_t}^{\text{ch}} + I_{n,k_t}^{\text{dch}} \le 1, \ \forall n \in \mathcal{E}, \forall k_t \in \mathcal{T}, \quad (17)$$

Spinning Reserve Constraint:

$$\sum_{g \in \mathcal{G}} (P_g^{\text{max}} - P_{g,k_t}) \Theta_{g,k_t} \ge RES_{k_t}, \ \forall k_t \in \mathcal{T}, \quad (18)$$

Constraint on the Lines' Power Flow:

$$S_{i,j,k_t}(|V_i|, |\delta_i|, |V_j|, |\delta_j|) \le S_{i,j}^{\text{max}}, \ \forall i,j \in \mathcal{B}, \quad (19)$$

Constraint on Voltage Limits Related to Power Flow:

$$V^{\text{min}} \le V_{i,k_t} \le V^{\text{max}}, \ \forall k_t \in \mathcal{T}, \quad (20)$$

III. Problem Formulation of the Proposed Cyberattacks-Tolerant Tertiary Control in the FIPES

This section mathematically details the proposed cyberattacks-tolerant tertiary control, which is based on IGDT methodology. Therefore, the considered Hypothesis is first described before providing the proposed approach's details.

Hypothesis. *When a data integrity attack—either a severe or negligible (equivalently undetectable) attack one—occurs,* *there is a change in the operating cost of OC. This amount of change [in percentage or per unit (pu)] is formulated by a variable named δ_{CA} in this paper, which is defined as the tolerable increment in operating cost considering the vulnerability of tertiary controls to cyberattacks. For **Severe Data Integrity Attacks**, the "new" operating cost of OC^{new} is considered, and the optimization process ensures that it is "below" $(1+\delta_{CA})OC^{*}$, or equivalently, the change in the new operating cost is less that $\delta_{CA} \times 100\%$. In $(1+\delta_{CA})OC^{*}$, OC^{*} is the operating costs without any attacks (presented in Section II). Therefore, it is possible to find the random "RoU"s associated with various entities if targeted by CA. That random RoU is regarded as an uncertain piece of information that is handled by the IGDT methodology when considered in the IGDT-based tertiary control. Subsequently, by finding the maximum RoU, while considering the constraint of $OC^{new} \leq (1+\delta_{CA}) \times OC^{*}$, it is feasible to "quantify" the amount of change in the operating cost of OC provided that severe data integrity attacks happen. For **Negligible Data Integrity Attacks**, a similar maximizing problem is considered, but there are additional constraints on each of the RoUs associated with all entities constructing the MMGs' FIPES. Those extra constraints will be limited to small values (during the maximization process) so that negligible data integrity attacks are taken into account.*

According to the Hypothesis above, the IGDT approach is the key to the method proposed in this article. Then, Subsection III-A briefly elaborates on the concepts behind the IGDT methodology. Afterward, Subsection III-B thoroughly expresses the mathematics required for formulating this research's Hypothesis. Finally, Subsection IV provides the outcomes to support the Hypothesis described here.

A. IGDT Approach

The uncertain systems, for which the statistical data of uncertain parameters is unavailable, are well-managed by the IGDT [40]. Various approaches can be adopted in the IGDT. They include risk-averse strategy and risk-taking strategy. In the former, the decision maker tries to minimize the operation risk, while in the the latter, the objective is to maximize the profit via minimizing variable operating costs. In the risk-averse approach, uncertainty negatively impacts the system, and an appropriate robustness band should be defined to achieve a safer operation [40]. In this paper, the risk-averse strategy, in which the uncertainty increases the operating cost, is employed to determine the robustness regions of uncertain parameters.

The uncertainty can be expressed in two different aspects because the uncertainty-made deviations are either favorable or adverse. Adversity increases the possibility of failure, while the opportunity to succeed is referred to as favorability. In the IGDT, "immunity functions" are abel to present negative or positive effects of uncertainty. A robustness function defined the immunity to failure. The robustness function—i.e., robustness band—is the uncertainty's largest amount for which the occurrence of failure is impossible. Let us assume that $\Pi(\chi_{k_t}, \varphi_{1,k_t}, \varphi_{2,k_t}, ..., \varphi_{n,k_t})$ denotes the system model, indicating the input/output structure of the system. Besides, χ_{k_t} is the set of decision variables at each time interval, while φ_{z,k_t} denotes the system's uncertain parameters. In the IGDT, various ways are able to express uncertain parameters, as described in [40]. This research uses the envelope bound model as follows.

$$\varphi_{z,k_t} \in \psi_{z,k_t}(\kappa_z, \tilde{\varphi}_{z,k_t}),\ \forall z \in \mathcal{Z}, \forall k_t \in \mathcal{T},$$
$$\psi_{z,k_t}(\kappa_z, \tilde{\varphi}_{z,k_t}) = \left| \frac{\varphi_{z,k_t} - \tilde{\varphi}_{z,k_t}}{\tilde{\varphi}_{z,k_t}} \right| < \kappa_z, \tag{21}$$

where φ_{z,k_t} denotes the system's z^{th} uncertain parameter; $\tilde{\varphi}_{z,k_t}$ describes its predicted value; $\psi_{z,k_t}(\kappa_z, \tilde{\varphi}_{z,k_t})$ indicates the set of all φ_{z,k_t}'s values; and κ_z shows the uncertain parameter z's uncertainty horizon.

The uncertainty horizon's largest value, in which all system's minimum requirements remain satisfied, expresses the decision vector χ_{k_t}'s robustness. Consequently , it can be formulated as

$$\tilde{R}_z = \max_{\kappa_z} \{\kappa_z\},\ \forall z \in \mathcal{Z},$$
$$\min_{\varphi_{z,k_t} \in \psi_{z,k_t}(\kappa_z, \tilde{\varphi}_{z,k_t}), \forall z \in \mathcal{Z}, \forall k_t \in \mathcal{T}} \left\{ \Pi(\chi_{k_t}, \varphi_{1,k_t}, \varphi_{2,k_t}, ..., \varphi_{n,k_t}) \right\} > \Pi_{min}, \tag{22}$$

where $\tilde{R}_z$ is the uncertain parameter z's robustness band, and Π_{min} is the set of all system's minimum requirements.

B. Proposed Mathematical Formulation with Cyberattack Impacts

In the proposed CT^{2}C (which uses IGDT employed in the FIPES of MMGs), the goal is to reduce the operating cost of the MMG, i.e., the function of OC considering the 24-hour energy consumption, not only the power consumption. This methodology allows for better energy management related to the OC of MMG. This OC is the cost of operation for different time intervals associated with generating units. During this process, all equality and inequality constraints that consider power flow and technical limitations related to the operation of different generating units will be taken into account.

1) Without Any Limits on RoUs to Consider Severe Data Integrity Attacks: In this part, "sever" data integrity attacks are considered. In this regard, there are no limits on RoUs so that they can take and reach any numbers during the optimization process. In other words, the optimization process is more relaxed compared to the next subsection. To this end, Subsubsection III-B1 proposes two key, integral steps as follows. It is noteworthy that this subsubsection will be vital to the next one, which takes into account a limit on RoUs so that negligible (or extremely non-detectable) attacks are seen (or undetectable attacks) as well.

Stage A—In the first stage, (2)–(20) are able to determine the minimum OC over 24 hours with a step size of one hour. Therefore, (2)–(20) provide the generation amounts for the one-hour time intervals, which is flexible and can be altered. In other words, they provide all the generation amounts, including BESSs, in addition to the OC for 24 hours reflecting the energy generation's OCs and the operating costs of OC^{*}. In other words, OC^{*} conveys the MMG's operating costs—when

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JESTPE.2020.3015447, IEEE Journal of Emerging and Selected Topics in Power Electronics

there are not any data integrity attacks by CAs. Then, any data integrity attacks will cause the OC^* to be increased. Stage B is able to capture that part in a mathematically efficient way.

Stage B—In the second stage, (23)–(37) are able to take into account the data integrity attacks' effect on the tertiary control of the FIPES using the CT^{2}C proposed here. In this regard, this work supposes that the CAs cause an increase in the OC^* with δ_{CA} as the tolerable increment in operating costs considering the vulnerability of the tertiary control to data integrity attacks. This consideration leads to a new OC^{new} describing the impact of CAs by employing a portion of OC^* calculated in the first stage—described by (24). Equation (24) mathematically states that if one wants to keep the newly impacted OC below the amount calculated in Stage A, how much deviation could have happened in the amount of generation (and/or load), supposing that data integrity attack has been injected into the amounts communicated via the FIPES's tertiary controls. This way, OC^{new}, which is the OC impacted by CAs, is kept below $(1+\delta_{\text{CA}}) \times 100\%$. OC^{new} is able to tell engineers about this statement that "if the OC is increased by δ_{CA}, what will the new generation (and/or load) be, and thereby, by how much should the new generation (and/or load) be increased?" In other words, given δ_{CA}, the new generation amounts can be found by an RoU. One is able to calculate the RoU for all units associated with the generation, load, BESS, etc. in the FIPES's structure. Afterward, the RoUs associated with all of the entities above are maximized using IGDT to find the most vulnerable PoCAs considering the amount of increase in OC. As shown in (23), K_{DG}, K_{BESS}, K_{PV}, K_{WT}, and K_{Load} are the aforementioned RoUs related to diesel generating units [or equivalently diesel gensets (DGs)], BESS units, photovoltaic (PV) units, wind turbine (WT) units, and loads, respectively. Next, (30)–(37), which are the appropriately updated versions of (1)–(16), are able to deal with the new generation amount affected by RoUs. Consequently, they mathematically consider the influence of CAs on the tertiary control of the FIPES.

Now, as described above in ***Stage A*** and ***Stage B***, in the second level of modeling, the effect of CAs is considered by employing an additional uncertain variable that is able to take into account the data integrity attack by CAs. Then, the new variable—which is able to model the effect of CAs on the OC mathematically—results in the following equations. They include a "new" OC, as well as constraints regarding CAs. With respect to all of the constraints, (23) is the critical part that is able to handle the CAs' impact on the tertiary control of FIPES by maximizing the RoU as follows.

$$\text{Maximize } RoU = \sum_{g\in\mathcal{G}} P_{g,k_t} K_{\text{DG}} + \sum_{n\in\mathcal{E}} P^{\text{dch}}_{n,k_t} K_{\text{BESS}} + \sum_{i\in\mathcal{B}_{\text{PV}}} PV_{i,k_t} K_{\text{PV}} + \sum_{j\in\mathcal{B}_{\text{WT}}} PW_{j,k_t} K_{\text{WT}} + \sum_{l\in\mathcal{B}_L} PD_{l,k_t} K_{\text{Load}}, \tag{23}$$

Subject To:

Constraint on Maximum Impact of Data Integrity Attacks on the Operating Cost of OC:

$$OC^{\text{new}} \le (1+\delta_{\text{CA}}) OC^*, \tag{24}$$

Constraint on the Impact of Data Integrity Attacks on Diesel Gensets:

$$P^{\text{new}}_{g,k_t} = (1-K_{\text{DG}}) P_{g,k_t} \forall g \in \mathcal{G}, \forall k_t \in \mathcal{T}, \tag{25}$$

Constraint on the Impact of Data Integrity Attacks on Wind Turbine Generations:

$$PW^{\text{new}}_{j,k_t} = (1-K_{\text{WT}}) PW_{j,k_t} \forall j \in \mathcal{B}_{\text{WT}}, \forall k_t \in \mathcal{T}, \tag{26}$$

Constraint on the Impact of Data Integrity Attacks on Photovoltaic Systems:

$$PV^{\text{new}}_{i,k_t} = (1-K_{\text{PV}}) PV_{i,k_t} \forall i \in \mathcal{B}_{\text{PV}}, \forall k_t \in \mathcal{T}, \tag{27}$$

Constraint on the Impact of Data Integrity Attacks on Battery Energy Storage Systems:

$$P^{\text{dch,new}}_{n,k_t} = (1-K_{\text{BESS}}) P^{\text{dch}}_{n,k_t} \forall n \in \mathcal{E}, \forall k_t \in \mathcal{T}, \tag{28}$$

Constraint on the Impact of Data Integrity Attacks on Loads:

$$PD^{\text{new}}_{l,k_t} = (1+K_{\text{Load}}) PD_{l,k_t} \forall l \in \mathcal{B}_L, \forall k_t \in \mathcal{T}, \tag{29}$$

New *Operating Cost OC^{new}:*

$$OC^{\text{new}} = \sum_{k_t\in\mathcal{T}} \sum_{g\in\mathcal{G}} [\{(a_g (S_{base} P^{\text{new}}_{g,k_t})^2 + b_g (S_{base} P^{\text{new}}_{g,k_t})) + C_g \Theta_{g,k_t}\} \Delta t_{k_t} + C^{\text{sup}}_g \mu_{g,k_t} + C^{\text{sdn}}_g \lambda_{g,k_t}], \tag{30}$$

New *Active Power Balance:*

$$\sum_{g\in\mathcal{G}_i} (P^{\text{new}}_{g,k_t} \Theta_{g,k_t}) + PW^{\text{new}}_{i,k_t} + PV^{\text{new}}_{i,k_t} - PD^{\text{new}}_{i,k_t} + \sum_{n\in\mathcal{E}} (P^{\text{dch,new}}_{n,k_t} - P^{\text{ch,new}}_{n,k_t}) = \sum_{j\in\mathcal{B}} V_{i,k_t} V_{j,k_t} Y_{i,j} \cos(\theta_{i,j} + \delta_{j,k_t} - \delta_{i,k_t}) \forall i, j, \forall k_t, \tag{31}$$

New *Aeactive Power Balance Equation (Only in the AC Side):*

$$P^{\min}_g \Theta_{g,k_t} \le P^{\text{new}}_{g,k_t} \le P^{\max}_g \Theta_{g,k_t}, \quad \forall g \in \mathcal{G}, \forall k_t \in \mathcal{T}, \tag{32}$$

New *Ramp-up Rate of Generating Units:*

$$P^{\text{new}}_{g,k_t+\Delta t_{k_t}} - P^{\text{new}}_{g,k_t} \le R^{\text{up}}_g \Delta t_{k_t} + \mu_{g,k_t+\Delta t_{k_t}} P^{\min}_g, \quad \forall g \in \mathcal{G}, \forall k_t \in \mathcal{T}, \tag{33}$$

New *Ramp-down Rate of Generating Units:*

$$P^{\text{new}}_{g,k_t} - P^{\text{new}}_{g,k_t+\Delta t_{k_t}} \le R^{\text{dn}}_g \Delta t_{k_t} + \lambda_{g,k_t+\Delta t_{k_t}} P^{\min}_g, \quad \forall g \in \mathcal{G}, \forall k_t \in \mathcal{T}, \tag{34}$$

New *BESS's SOC's Equation Using Charging/Discharging Power and Efficiency:*

$$SOC^{\text{new}}_{n,k_t+\Delta t_{k_t}} - SOC^{\text{new}}_{n,k_t} = [P_{n,k_t} \eta^{\text{ch}}_n - \frac{P^{\text{dch,new}}_{n,k_t}}{\eta^{\text{dch}}_n}] \Delta t, \quad \forall n \in \mathcal{E}, \forall k_t \in \mathcal{T}, \tag{35}$$

New *SOC Lower and Upper Bounds of the BESSs:*

$$SOC^{\min}_n \le SOC^{\text{new}}_{n,k_t} \le SOC^{\max}_n \forall n \in \mathcal{E}, \forall k_t \in \mathcal{T}, \tag{36}$$

New *BESS's Maximum Discharging Power:*

$$0 \le P^{\text{dch,new}}_{n,k_t} \le P^{\max}_{BESS_n} I^{\text{dch}}_{n,k_t} \forall n \in \mathcal{E}, \forall k_t \in \mathcal{T} \tag{37}$$

Consequently, by considering CAs in the tertiary control of FIPES using the CT^{2}C proposed in (23)–(37), this research is able to find the most susceptible PoCAs mathematically. Those PoCAs are associated with all entities forming the FIPES, not

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JESTPE.2020.3015447, IEEE Journal of Emerging and Selected Topics in Power Electronics

only for the generating units but also for the loads. They can dramatically influence the operating costs of an MMG with an FIPES structure, and the RoUs defined above are able to describe the susceptibility of various entities to CAs. Indeed, if the CA impacts a given entity with the RoU, its impact on the operating cost is not higher than δ_{CA}. It means that "the higher" the RoU, "the lesser" the effect on the FIPES's tertiary control caused by CAs. This statement will be true because the effect of changes in the amount of generation/consumption within the RoU is not higher than δ_{CA}. In order to display the proposed method in this subsection, Fig. 3 shows the flowchart of the detailed process explained above using a stepwise process.

2) With Limits on RoUs to Consider Negligible Data Integrity Attacks: In this part, studies associated with the negligible data integrity attacks—regarded as extremely non-detectable CAs (or equivalently undetectable CAs)—have been provided. To this end, in direct contrast to what has been done in Subsubsection III-B1, there do exist limits on RoUs. Consequently, they should now be regarded as "new" constraints in the optimization process. In other words, the optimization process is not as relaxed as what is in the earlier subsection. In this regard, K_{DG}, K_{BESS}, K_{PV}, K_{WT}, and K_{Load} are included in the constraints of (38)–(42) in this subsubsection as follows. In (38)–(42), $K_{\text{DG}}^{\max}$, $K_{\text{BESS}}^{\max}$, $K_{\text{PV}}^{\max}$, $K_{\text{WT}}^{\max}$, and $K_{\text{Load}}^{\max}$ are selected according to the minimum effect that data integrity attacks should have on operating costs. Obviously, the less they are selected to be, the higher cybersecurity investments should be made. In this subsection, the values of 1%, 2%, 3%, and 4% are selected for $K_{\text{DG}}^{\max}$, $K_{\text{BESS}}^{\max}$, $K_{\text{PV}}^{\max}$, $K_{\text{WT}}^{\max}$, and $K_{\text{Load}}^{\max}$ as they show very less impact caused by data integrity attacks via CAs. All can be equal without loss of generality here. In this subsection, because of the fact that higher resolutions are required, the 5-minute time intervals (equal to 288 intervals during a 24-hour time window) are considered. In order to demonstrate the proposed approach in this subsection, illustratively, Fig. 4 shows the flowchart of the detailed process explained above using a stepwise methodology.

Constraint on Diesel Gensets' RoUs:

$$K_{\text{DG}} \le K_{\text{DG}}^{\max}, \tag{38}$$

Constraint on Photovoltaic Systems' RoUs:

$$K_{\text{WT}} \le K_{\text{WT}}^{\max}, \tag{39}$$

Constraint on Wind Turbine Generations' RoUs:

$$K_{\text{PV}} \le K_{\text{PV}}^{\max}, \tag{40}$$

Constraint on Battery Energy Storage Systems' RoUs:

$$K_{\text{BESS}} \le K_{\text{BESS}}^{\max}, \tag{41}$$

Constraint on Loads' RoUs:

$$K_{\text{Load}} \le K_{\text{Load}}^{\max}, \tag{42}$$

IV. Outcomes and Considered Case Studies

A CIGRE microgrid test system is employed to simulate the results and find the outcomes of the proposed IGDT-based tertiary control [41], as depicted in Fig. 5. This CIGRE microgrid is a big, multi-busbar microgrid. It also features an FIPES and requires considerable communication infrastructure

TABLE I
Data for the Microgrid Diesel Gensets in Fig. 5.

Parameter	DG #1	DG #2	DG #3	DG #4	DG #5
a_g [\$/(kWh)^2]	0.00015	0.00025	0.00015	0.00010	0.0005
b_g [\$/kWh]	0.2881	0.2876	0.2571	0.224	0.3476
c_g [\$/h]	7.5	0	25.5	45.5	0
c_g^{sup} [\$]	15	7.35	45	95	10
c_g^{sdn} [\$]	5.3	1.44	8.3	15.3	0
R_g^{up} [kW/h]	2000	600	1800	3200	450
R_g^{dn} [kW/h]	3500	1500	3000	4000	1000
$P_g^{\max}$ [kW]	5000	1500	4000	6000	1000
$P_g^{\min}$[kW]	180	100	150	200	100

for its operation to be utilized as an MMG. It consists of diesel generating units (or equivalently diesel gensets), BESS units, WTs, and PV systems.

It has a total capacity of 26.50 MW, whose details are as follows. The total installed capacities of the diesel gensets [five units (three of which have been connected to Bus #B1), WTs (three units), and PV systems (eight units) are 17500, 8000, and 1000 kW, respectively. Besides, it has been equipped with two battery energy storage systems—totaling 2000 kW. Table I provides the data of diesel gensets used in this work. Other typical parameters associated with grid components, such as BESS units, WTs, PV units, and so forth, are available in Fig. 5. Note that because the "performance" of the forecasting system is not within the scope of this paper, the proposed IGDT-based tertiary control is intended to (and is able to) work with the output of any forecasting system with adequate performance.

A. Proposed Method's Results for Severe Data Integrity Attacks

The proposed IGDT-based algorithm (shown in Fig. 3) is employed in the tertiary control of the FIPES using a General Algebraic Modeling System (GAMS), a high-level modeling system for mathematical optimization [42]. The model is a mixed-integer nonlinear programming (MINLP) problem, so the GAMS' MINLP solver can solve it. The GAMS modeling system has been running on an Intel® CPU Core i7-4700HQ 2.4 GHz PC with 8 GB of RAM. It has run the optimization algorithm by the MINLP solver in non-real-time using C++, and it has been installed on the Windows 10 operating system. Note that, here, finding the globally optimal solutions has been guaranteed [43].

The data of the CIGRE microgrid test system in Fig. 5 is used in order to demonstrate the outcomes of the proposed IGDT-based tertiary control described in Subsubsection III-B1. Solving the proposed model in a 24-hour time window with a step size of one hour is considered here. This subsection comprehensively considers several scenarios, including various values regarding δ_{CA} and different PoCAs, i.e., different generating units, load sections, and both. Table II summarizes those scenarios; scenarios S_{1x}, and S_{2x}, and S_{3x} are related to the inclusion of both generating units and load sections, only generating units, and only load sections, respectively—where $x \in \{1, ..., 6\}$ shows the number with respect to the amount

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JESTPE.2020.3015447, IEEE Journal of Emerging and Selected Topics in Power Electronics

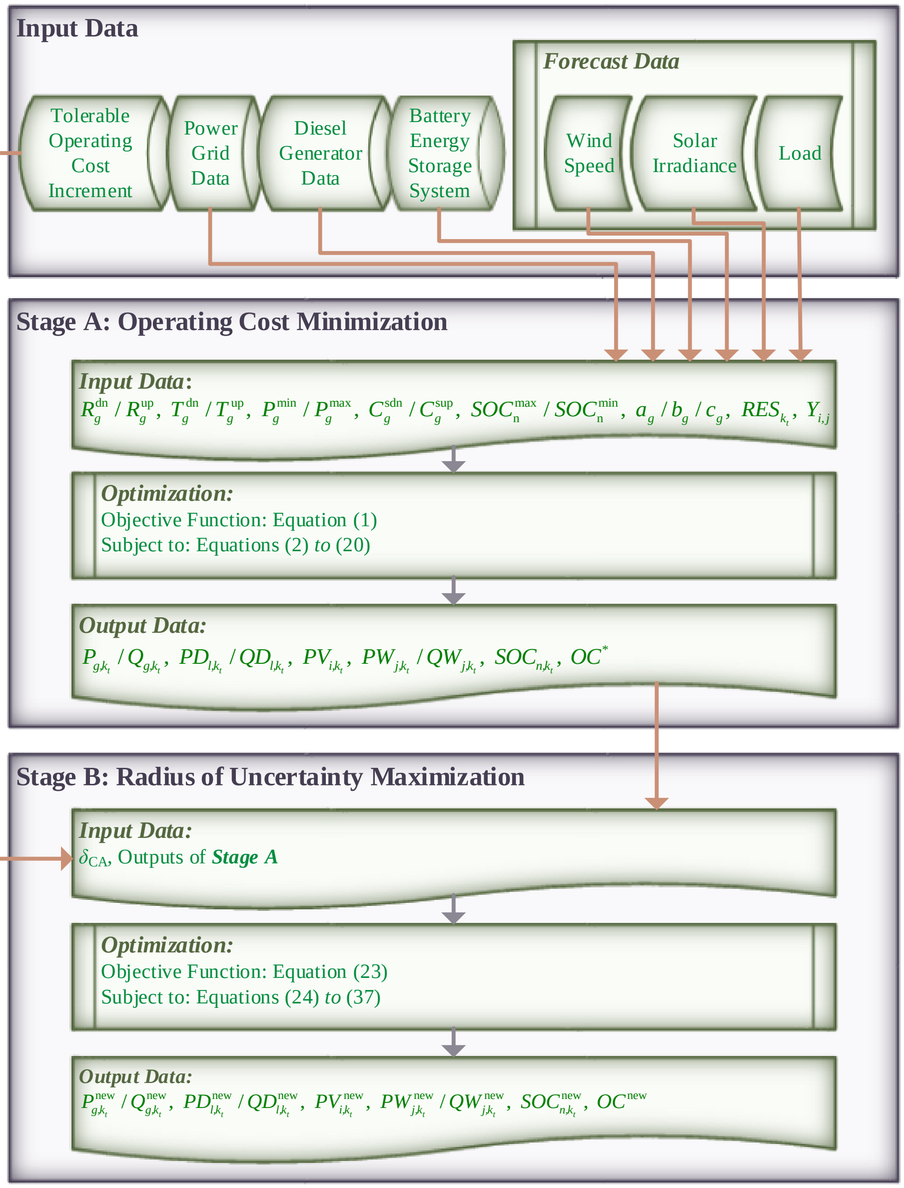

Fig. 3. Flowchart of the proposed approach of CT^{2}C using stepwise methodology in Subsubsection III-B1.

of δ_{CA} in %. Figs. 6–11 depict the thorough outcomes of the CT^{2}C proposed in this subsection.

B. Proposed Method's Results for Negligible Data Integrity Attacks

Similarly, the proposed IGDT-based algorithm (shown in Fig. 4) is employed in the tertiary control of the FIPES using GAMS again [42]. Again, the GAMS modeling system has been running on an Intel® CPU Core i7-4700HQ 2.4 GHz PC with 8 GB of RAM. Likewise, it has run the optimization algorithm by the MIQCP solver in non-real-time using C++, and it has been installed on the Windows 10 operating system. Note that, here, finding the globally optimal solutions has been guaranteed as well [43].

The data of the CIGRE microgrid test system in Fig. 5 is used in order to demonstrate the outcomes of the proposed IGDT-based tertiary control presented in Subsubsection III-B1. Because of considering "negligible" (or non-detectable) data integrity attacks, solving the proposed methodology in a 24-hour time window with a step size of five minutes is considered here. This subsection comprehensively considers all scenarios, including very small values regarding δ_{CA} and different PoCAs, i.e., both different generating units and load sections. Table III summarizes the natural numbers that assigned to different entities (i.e., various generating units and loads) and used in the outcomes. The scenarios S_{4x} (reported in Table IV) are related to the inclusion of both generating units and load section—where $x \in \{1, ..., 4\}$ shows the number with respect to the amount of maximum $RoUs^{\max}$ (in %) associated with $K_{\text{DG}}^{\max}$, $K_{\text{BESS}}^{\max}$, $K_{\text{PV}}^{\max}$, $K_{\text{WT}}^{\max}$, and $K_{\text{Load}}^{\max}$. Figs. 12 and 13 detail the outcomes of the CT^{2}C proposed in this subsection.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JESTPE.2020.3015447, IEEE Journal of Emerging and Selected Topics in Power Electronics

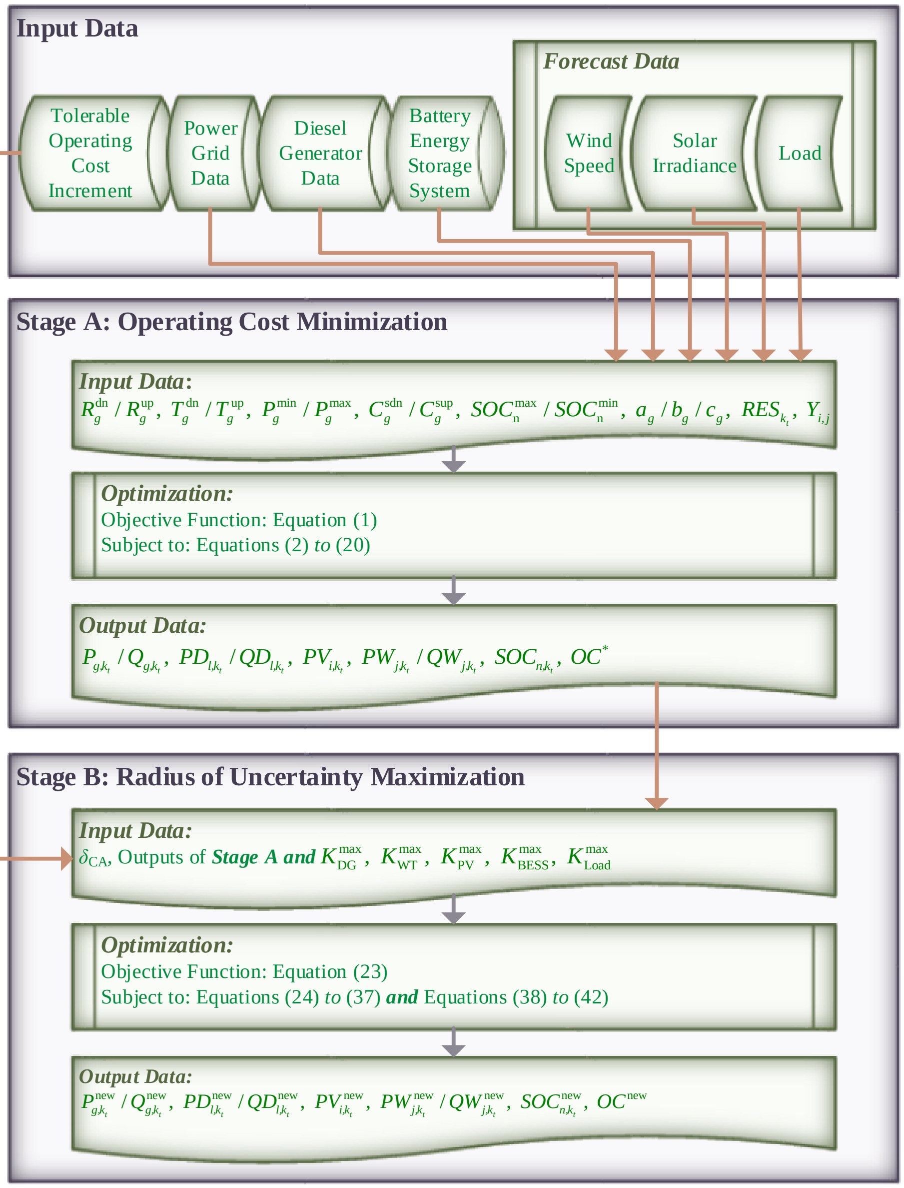

Fig. 4. Flowchart of the proposed approach of CT^{2}C using stepwise methodology in Subsubsection III-B2.

C. Discussions about the Results from the Proposed CT^{2}C

This subsection details the discussions about the results of the proposed algorithms for both severe and negligible uncertainties caused by data integrity attacks through the following subsections.

1) Proposed Method's Results for Severe Data Integrity Attacks: Figs. 6 and 7 reveal the CAs' impacts on the OC of tertiary control when S_{1x} scenarios happen. They are data integrity attacks affecting both generating units (i.e., those in Buses # $\underbrace{B1, B9, B13}_{\text{for DGs}}$; $\underbrace{B5, B6, B8}_{\text{for WTs}}$; $\underbrace{B3, B4, B5, B6, B8, B9, B10, B11}_{\text{for PVs}}$; and $\underbrace{B5, B10}_{\text{for BESSs}}$) and load sections (i.e., those in Buses $B2$, $B3$, $B4$, $B5$, $B6$, $B8$, $B10$, $B11$, $B12$, and $B13$). Those have been assigned to columns $\underbrace{C\#1, C\#2, C\#3}_{\text{for DGs}}$; $\underbrace{C\#4, C\#5, C\#6}_{\text{for WTs}}$; $\underbrace{C\#7, C\#8, C\#9, C\#10, C\#11, C\#12, C\#13, C\#14}_{\text{for PVs}}$; $\underbrace{C\#15, C\#16}_{\text{for BESSs}}$; $\underbrace{C\#17}_{\text{for Load @ B2}}$; $\underbrace{C\#18}_{\text{for Load @ B3}}$; $\underbrace{C\#19}_{\text{for Load @ B4}}$; $\underbrace{C\#20}_{\text{for Load @ B5}}$; $\underbrace{C\#21}_{\text{for Load @ B6}}$; $\underbrace{C\#22}_{\text{for Load @ B8}}$; $\underbrace{C\#23}_{\text{for Load @ B10}}$; $\underbrace{C\#24}_{\text{for Load @ B11}}$; $\underbrace{C\#25}_{\text{for Load @ B12}}$; $\underbrace{C\#26}_{\text{for Load @ B13}}$; in Fig. 6, respectively.

Fig. 6 shows the map associated with tertiary controls impacted for different hours of the 24-hour time window while Fig. 7 reveals the impacts for the entire day. Figs. 6 and 7 (the part assigned to $\delta_{CA} = 1\%$) show that, for the scope of the research under investigation and in the FIPES under study, the DGs are the first most susceptible PoCAs; the BESSs are the second most sensitive ones; the WTs are the third most

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JESTPE.2020.3015447, IEEE Journal of Emerging and Selected Topics in Power Electronics

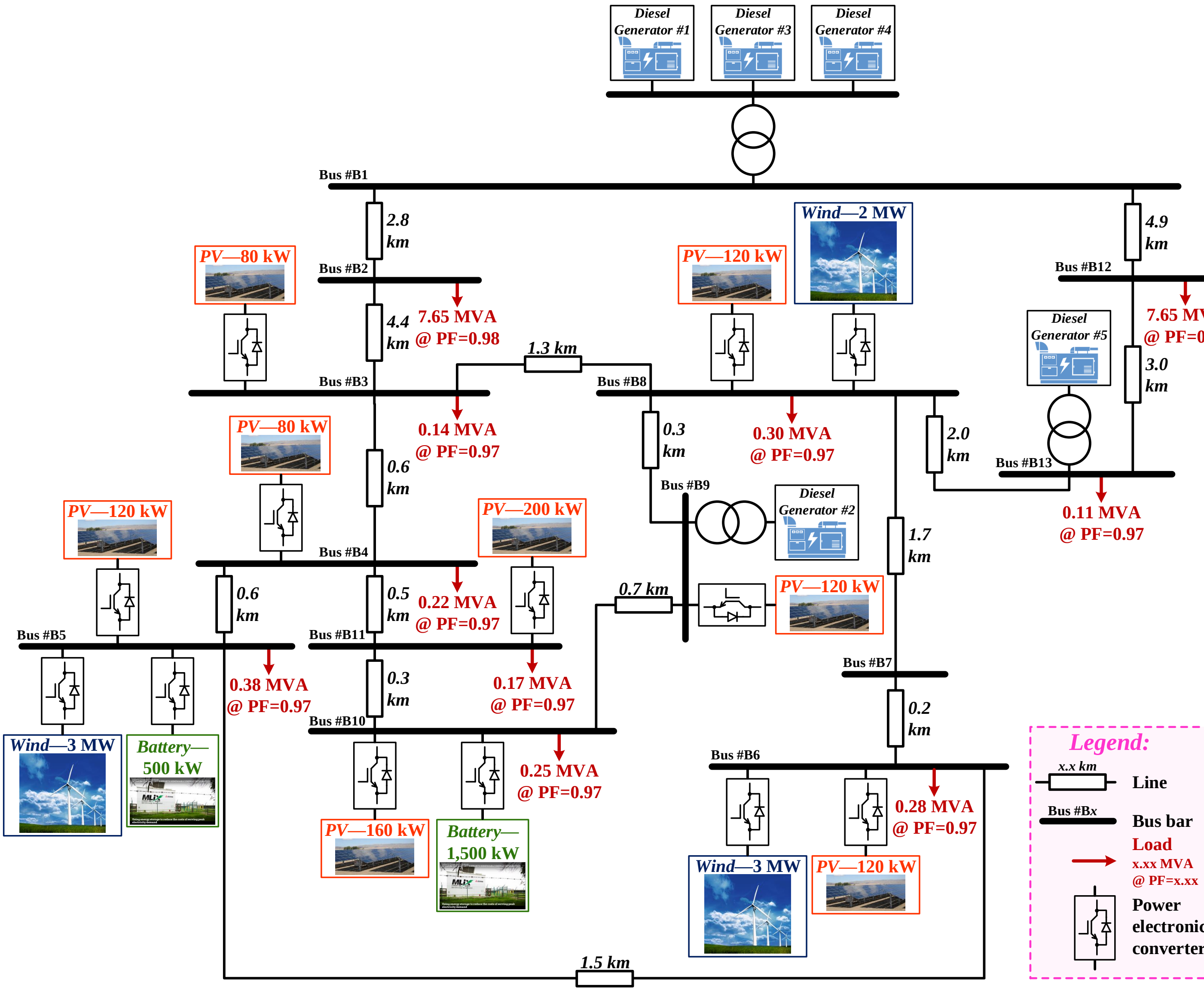

Fig. 5. Single-line diagram of the CIGRE microgrid benchmark [41].

vulnerable points; and the PVs are the least susceptible PoCAs. Figs. 8 and 9 reveal the same information regarding the CAs' impacts on the OC of tertiary control for the S_{2x} scenarios, in which CA injects data integrity attack into only generating units. Last, but by no means least, Figs. 10 and 11 reveal the impacts of CAS on the OC of tertiary control for the S_{3x} scenarios, in which CA injects data integrity attack into only the load sections. Figs. 10 and 11 demonstrate that the CAs in the load sections have almost the same impact on the OC of the tertiary control. However, the load close to DG #5 are more susceptible to CAs than other loads.

Finally, Fig. 14 has shown how the method proposed in Subsubsection III-B1 can be employed to invest money in cybersecurity enhancements of the FIPES of MMGs. Using a stepwise approach effectively provides designers with a flowchart to be able to compare the increases in operating costs (through a decrease in electrical energy efficiency caused by severe data integrity attacks) with the expenses of investments in cybersecurity.

2) Proposed Method's Results for Extremely Non-Detectable Data Integrity Attacks: Figs. 12 and 13 demonstrate the CAs' effects on the OC when S_{4x} scenarios happen. They are data integrity attacks influencing both generating units (i.e., those in Buses # $\underbrace{B1, B9, B13}_{\text{for DGs}}$; $\underbrace{B5, B6, B8}_{\text{for WTs}}$; $\underbrace{B3, B4, B5, B6, B8, B9, B10, B11}_{\text{for PVs}}$; and $\underbrace{B5, B10}_{\text{for BESSs}}$) and load sections (i.e., those in Buses $B2$, $B3$, $B4$, $B5$, $B6$, $B8$, $B10$, $B11$, $B12$, and $B13$). Those have been assigned to columns $\underbrace{C\#1, C\#2, C\#3}_{\text{for DGs}}$; $\underbrace{C\#4, C\#5, C\#6}_{\text{for WTs}}$; $\underbrace{C\#7, C\#8, C\#9, C\#10, C\#11, C\#12, C\#13, C\#14}_{\text{for PVs}}$; $\underbrace{C\#15, C\#16}_{\text{for BESSs}}$; $\underbrace{C\#17}_{\text{for Load @ B2}}$; $\underbrace{C\#18}_{\text{for Load @ B3}}$; $\underbrace{C\#19}_{\text{for Load @ B4}}$; $\underbrace{C\#20}_{\text{for Load @ B5}}$; $\underbrace{C\#21}_{\text{for Load @ B6}}$; $\underbrace{C\#22}_{\text{for Load @ B8}}$; $\underbrace{C\#23}_{\text{for Load @ B10}}$;

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JESTPE.2020.3015447, IEEE Journal of Emerging and Selected Topics in Power Electronics

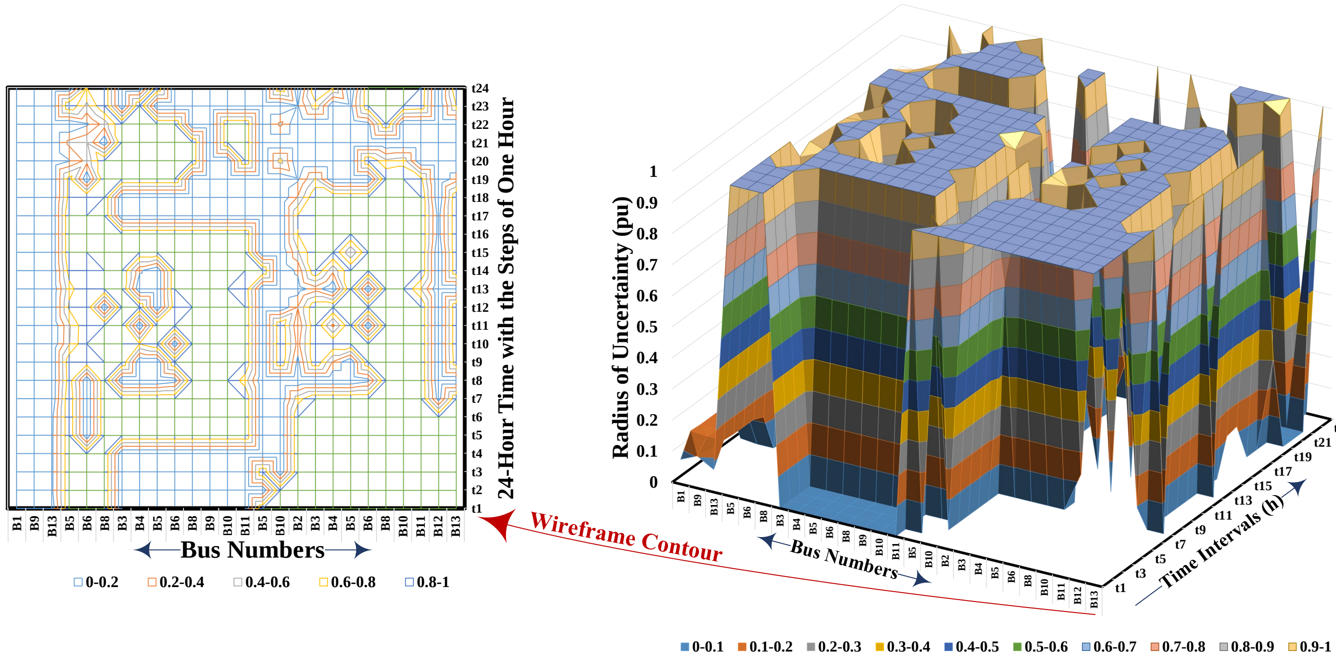

Fig. 6. Comparative results of scenario S_{11} within the 24-hour time window (with 1-hour intervals), presented as 3D surface and its wireframe contour—Fig. 7 has reported the entity's name associated with the individual natural number assigned to each Bus B# in the wireframe contour's X-axis.

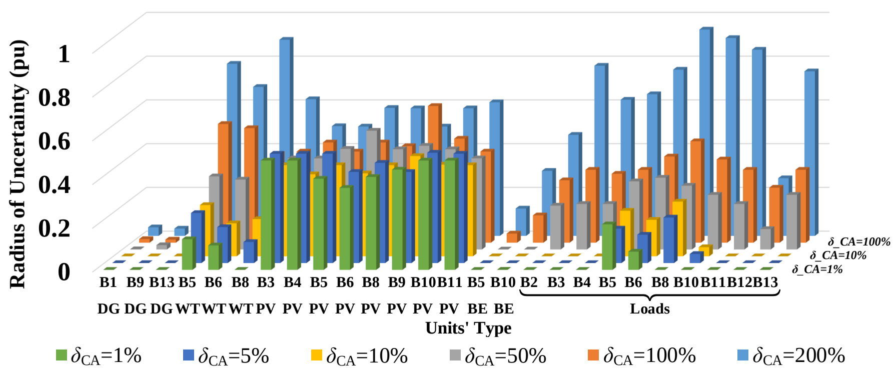

Fig. 7. Comparative results of scenarios S_{11}, S_{12}, S_{13}, S_{14}, S_{15}, and S_{16} for the entire 24 hours in the form of 3D columns (note that BE stands for battery energy storage system because of having insufficient space here).

$\underbrace{C\#24}_{\text{for Load @ B11}}$; $\underbrace{C\#25}_{\text{for Load @ B12}}$; $\underbrace{C\#26}_{\text{for Load @ B13}}$; in Figs. 12 and 13, respectively, as reported in Table III.

They illustrate the map associated with tertiary controls impacted for different hours of the 24-hour time window with 5-minute time intervals increasing the resolution. As Table IV details, the data integrity attacks—which have been considered by $RoU^{\max}$s of 4%, 3%, 2%, and 1%—increase the operating costs by 17%, 13%, 9%, and 4%, respectively—for sure, the lower $RoU^{\max}$, the higher cybersecurity investments are required. Also, Figs. 12 and 13 similarly show that, for the scope of the research under study and in the FIPES under investigation, the DGs are the first most susceptible PoCAs; the BESSs are the second most sensitive ones; the WTs are the third most vulnerable points; and the PVs are the least susceptible PoCAs.

Eventually, Fig. 15 has shown how the methodology elaborated in Subsubsection III-B2 can be used in investing funds in cybersecurity improvements of the FIPES of MMGs. Employing a stepwise method effectively provides designers with a flowchart to be able to make a comparison between the increases in operating costs (which are caused by negligible data integrity attacks) and the required money that should be invested in cybersecurity improvement.

D. Proposed Method's Practicability

This research has not contributed to the primary or zero-level control of a single converter (i.e., device-level controls) so that a single VSC is required to be tested. Also, it has not contributed to the secondary control of multiple, connected converters so that few VSCs are needed to be examined either. If this work is related to either case stated above, with the currently owned devices (e.g., the pieces of equipment applied in [3], [7], [15]), it will be practicable to conduct the tests associated with those controls using either a single converter or multiple ones. Instead, this work has, however, researched tertiary controls and studied the cyberattack's impacts on the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JESTPE.2020.3015447, IEEE Journal of Emerging and Selected Topics in Power Electronics

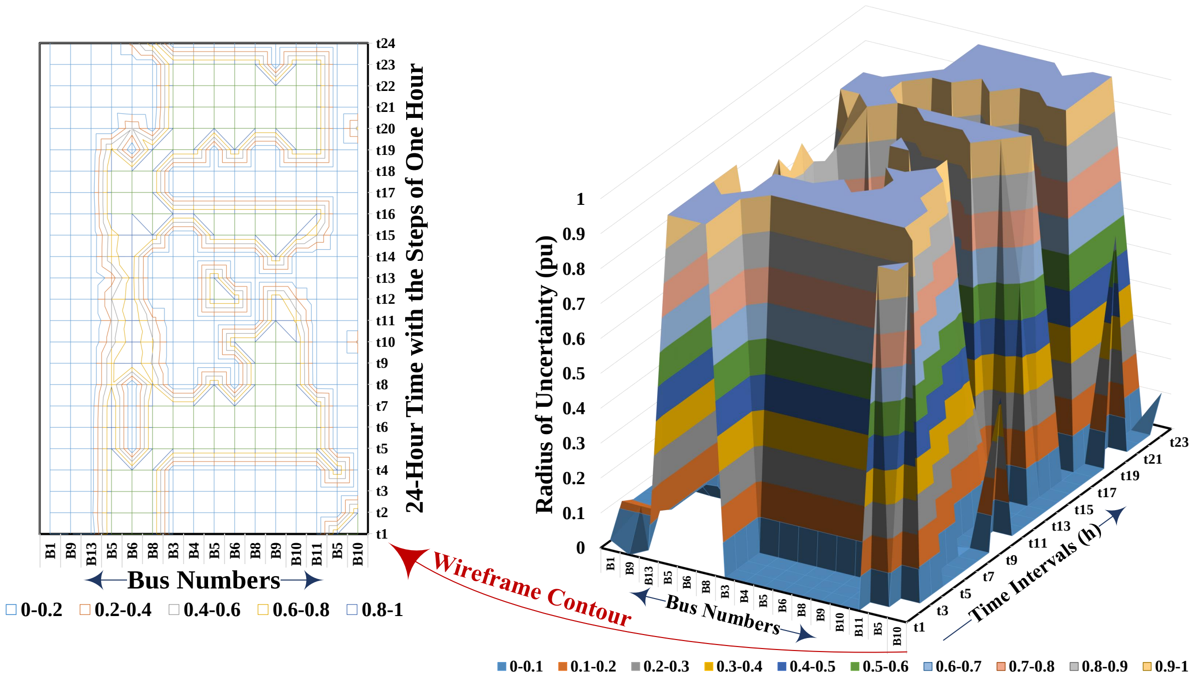

Fig. 8. Comparative results of scenario S_{22} within the 24-hour time window (with 1-hour intervals), presented as 3D surface and its wireframe contour—Fig. 9 has reported the entity's name associated with the individual natural number assigned to each Bus B# in the wireframe contour's X-axis.

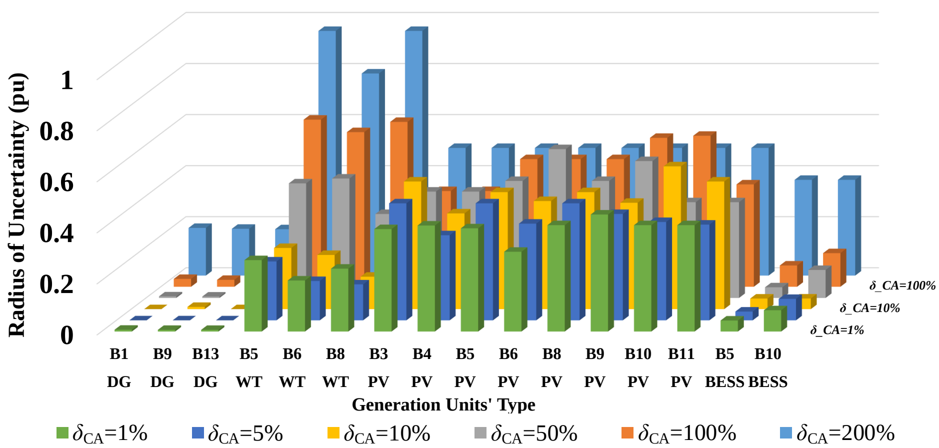

Fig. 9. Comparative results of scenarios S_{21}, S_{22}, S_{23}, S_{24}, S_{25}, and S_{26} for the entire 24 hours in the form of 3D columns.

microgrids' operating costs with the details mentioned in the article.

Moreover, in this research, it has been required to apply the per-unit numbers associated with operating costs—with the base of OC^* (i.e., operating costs for "without"-cyberattack conditions) as per this paper's contributions and requirements, which have been described in the write-up. Therefore, this paper's outcomes have been the increases in operating costs with respect to the base of OC^*.

On top of that, it has been dealing with a considerably huge microgrid—compared to the laboratory-scale facilities available to us—since there is a significant power system associated with the MMG under investigation. On the one hand, it is also true that making a pilot microgrid can be an option for experiments—but on the other hand, it is noteworthy that the facilities and the budget required for implementing such a microgrid make this alternative infeasible. All in all, it is impossible to achieve that system by physical devices considering our facilities. More importantly, based on this paper's scope, it is not required to arrange testing methods similar to what should be done for controlling a single converter or even a few (see [3], [7], [15]).

As a result, alternatively, the only possible option available to this work in order to assure readers that everything is implementable is real-time-simulation-based studies of such a system (including power components, controls, and so on.). This technique, which is based on real-time simulations, shows that it is feasible—as a proof of concept—or not. It will be utilized in many industrial and pilot projects before commissioning them in order to de-risk the implementation phase. As per the real-time simulation platform that is currently available to this work, the entire system is implementable in the NovaCor-based digital real-time simulation platform from *RTDS Technologies Inc.* [44].

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JESTPE.2020.3015447, IEEE Journal of Emerging and Selected Topics in Power Electronics

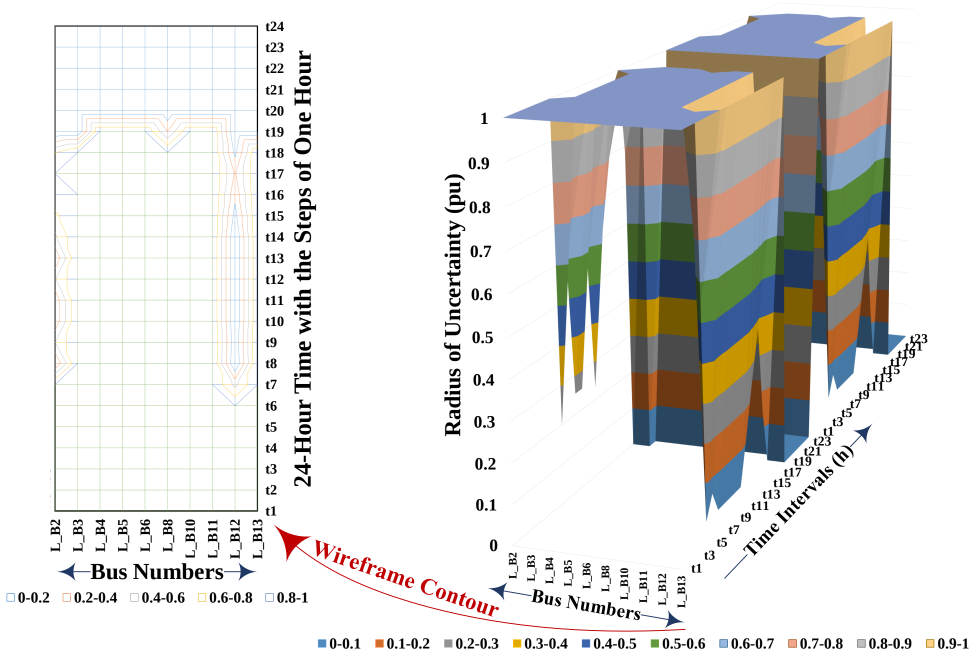

Fig. 10. Comparative results of scenario S_{33} within the 24-hour time window (with 1-hour intervals), presented as 3D surface and its wireframe contour—Fig. 11 has reported the entity's name associated with the individual natural number assigned to each Bus B# in the wireframe contour's X-axis.

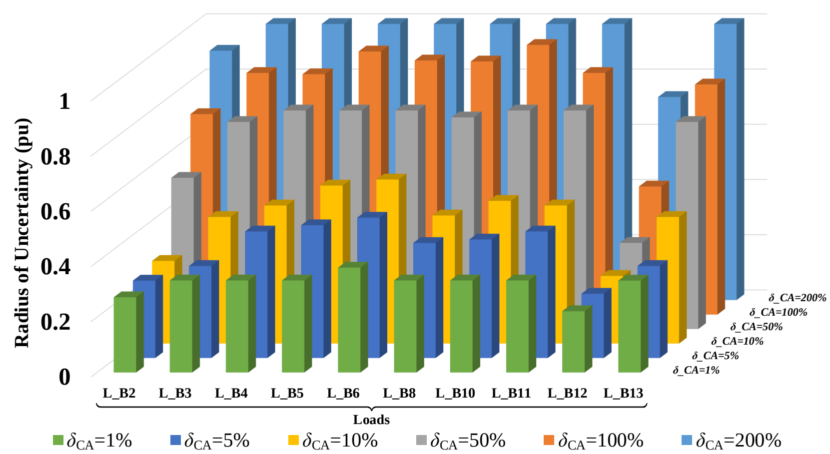

Fig. 11. Comparative results of scenarios S_{31}, S_{32}, S_{33}, S_{34}, S_{35}, and S_{36} for the entire 24 hours in the form of 3D columns.

Consequently, the implementation of such a system, including its controls, on an industrial digital real-time simulation platform (e.g., the NovaCor-based RTDS Platform here) reveals a proof of concept. In this regard, faulty signals (in percentage based on the nominal values) have been added to the measurement of each entity's active/reactive power. This action emulates and replicates the data integrity attack (via an "emulated" cyberattack with the presumed change in data), which impacts the measurements from those entities. In the arranged tests, the RoUs stated in Subsections IV-A and IV-B have been used, and δ_{CA} have been calculated and considered as per Subsubsections III-B1 and III-B2. Because of the fact that the RTDS Platform applies the same parameters for modeling the system as those of the model in Fig. 5, the power flows in both power networks are matched and become identical. As a consequence, the same results have been captured and obtained. Fig. 16 shows the detailed information on the above discussion.

One step further is that a new research and development (R & D) project is defined and proposed. In that R & D project, the real-time-simulated system portrayed above starts communicating with another system under "virtual" cyberattack (via an industrially emulated data integrity attack made by a third party). This process will also take advantage of one of the hardware-in-the-loop (HIL) techniques. Afterward, the data is captured for comparison purposes. The saved data is then analyzed for the cyberattack's influences on the operating costs and comparing them with the expenses required for cybersecurity investments.

Regarding the accurate implementation and practical aspects of the proposed approach, it is noteworthy that this part requires a separate, pilot R & D project based on flowcharts portrayed in Figs. 14 and 15. To this end, based on Figs. 14 and 15, a team of experts is required to provide the costs for improvements in the cybersecurity of the most susceptible points of attacks—elaborated in Subsubsections IV-C1 and

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JESTPE.2020.3015447, IEEE Journal of Emerging and Selected Topics in Power Electronics

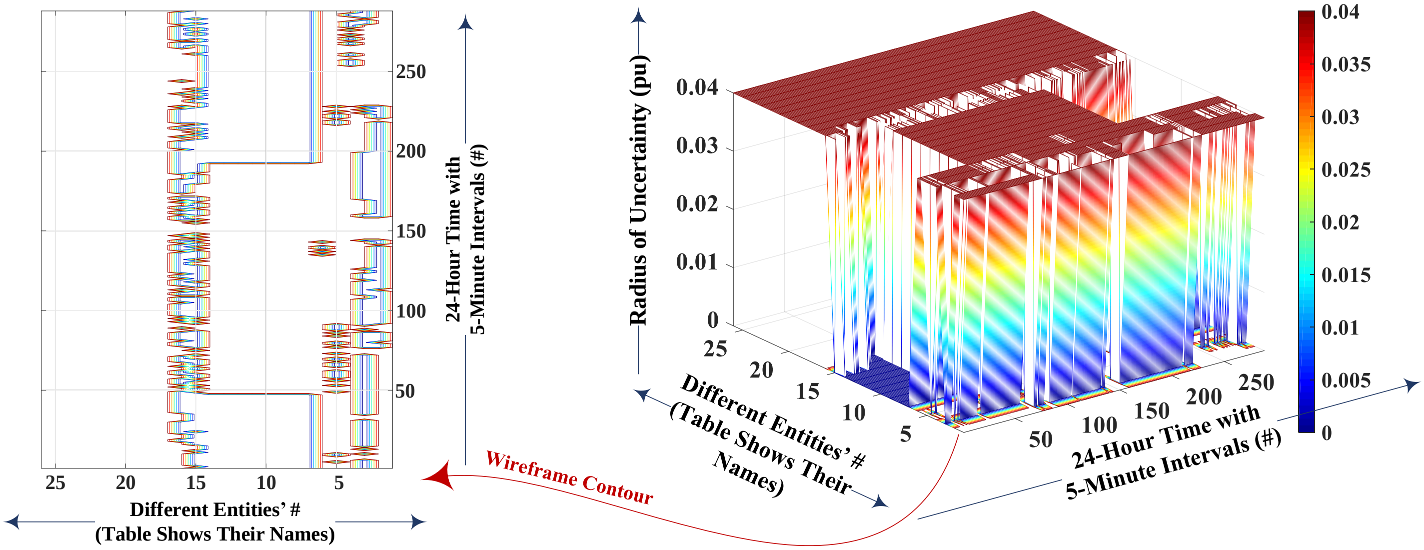

Fig. 12. Comparative results of scenario S_{4x} within the 24-hour time window (with 5-minute intervals), presented as 3D surface and its wireframe contour—Table III has reported the entity's name associated with the individual natural number assigned to each Bus B# in the wireframe contour's X-axis.

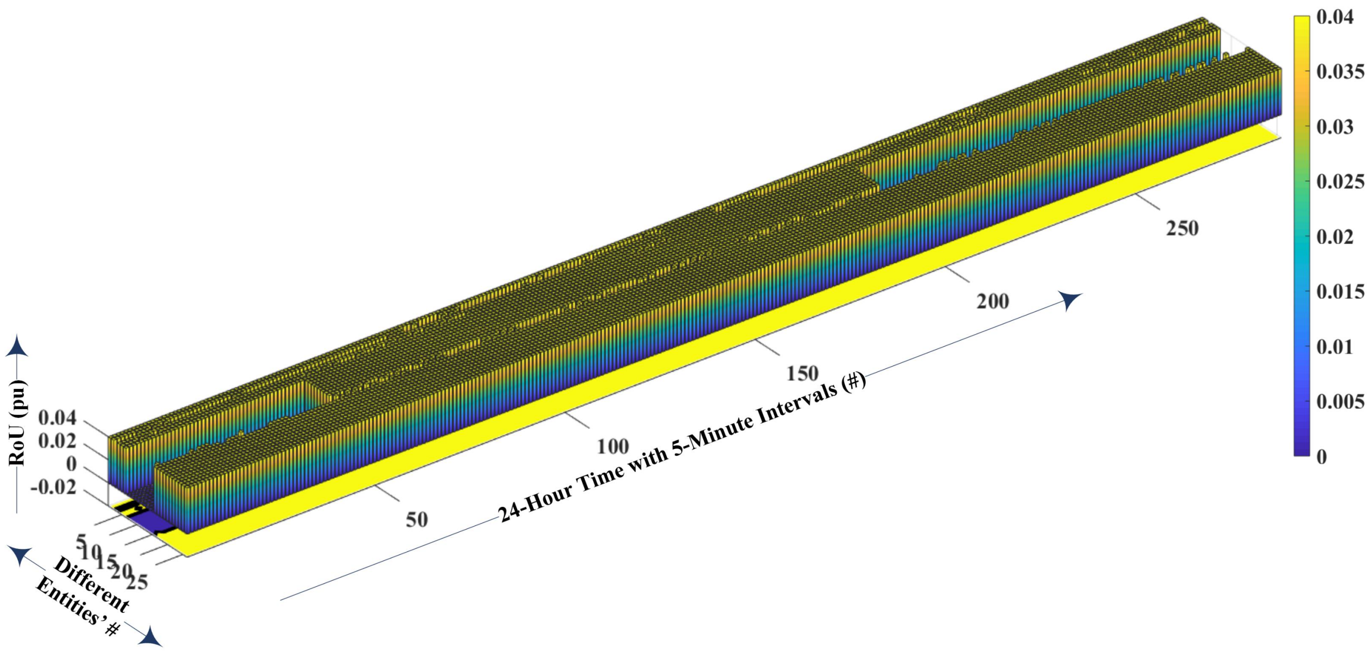

Fig. 13. Comparative results of scenarios S_{41}, S_{42}, S_{43}, and S_{44} for the entire 24 hours (with 5-minute intervals) in the form of 3D columns—Table III has reported the entity's name associated with the individual natural number assigned to each Bus B# in the 3D plot's Y-axis.

IV-C2. Equivalently, the expenses for the cybersecurity investments in those points are provided. Then, in order to ensure that the operating costs increase in less than $\delta_{\text{CA}} \times 100\%$, the expenses of cybersecurity investments in achieving such a security will be compared with those of the additional costs caused by cyberattacks (via data integrity attacks).

V. Conclusion

This paper has introduced a novel tertiary control methodology to consider both severe and negligible uncertainties caused by data integrity attacks into the tertiary controls of modernized microgrids. Those attacks have been increasing generation costs—or equivalently decreasing electrical energy efficiency. To this end, a hypothesis has been provided in the article; it has accounted for both severe data integrity attacks and negligible ones (may also be known as undetectable attacks). As elaborated in the hypothesis, the proposed approach is based on IGDT. The IGDT-based method has taken into account the cyberattacks' impacts on modernized microgrids' operating costs. This research has contributed to the field of tertiary control of the FIPES of MMGs as follows. 1) It has derived a tertiary control for the daily energy management that

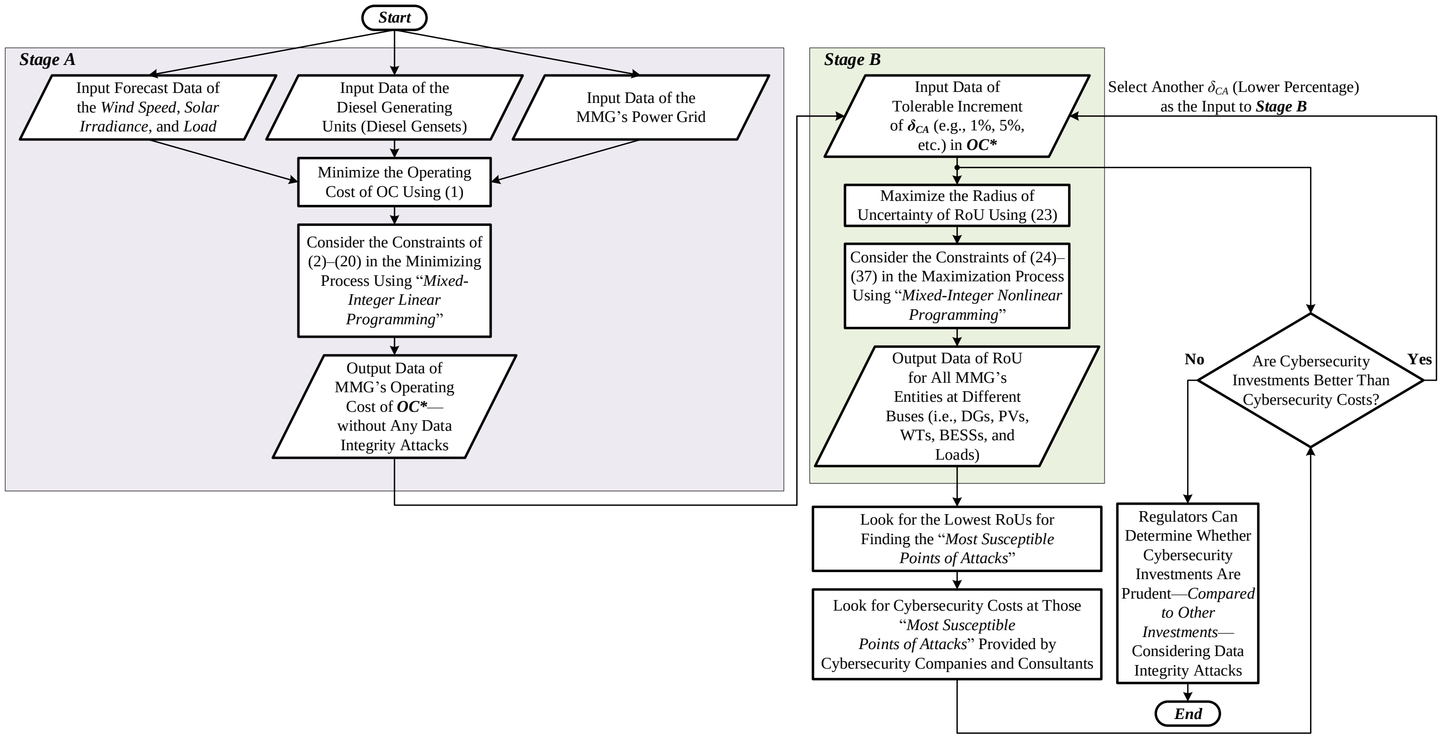

Fig. 14. Application of the proposed approach of CT^{2}C in Subsubsection III-B1 shown by the flowchart using a stepwise methodology.

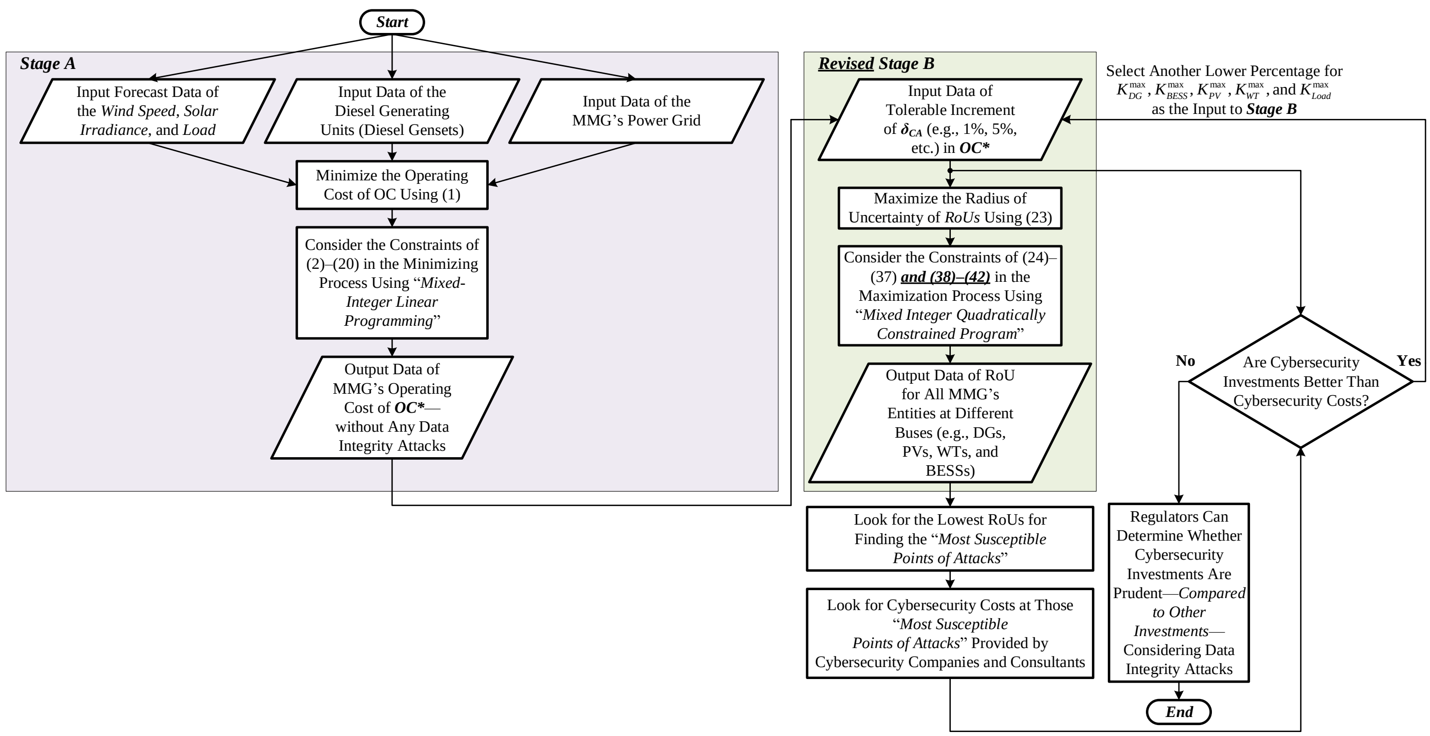

Fig. 15. Application of the proposed approach of CT^{2}C in Subsubsection III-B2 shown by the flowchart using a stepwise methodology.

optimally utilizes diesel generators, renewables, and battery energy storage systems. 2) It has mathematically modeled the cyberattacks into the optimization algorithm so that the most susceptible points of a cyberattack are found—concerning the operating costs of an MMG with the FIPES. 3) It has illustratively shown those pieces of information using appropriate maps and graphs. Illustrated by various flowcharts (stepwise methodologies), this paper's outcomes have also been able to inform design engineers of the investments in the MMGs' cybersecurity to ensure accuracy and economic optimization via an analytical and demonstrative approach.

Furthermore, the future work will include inspecting the FIPES-based MMG's power topology and finding its impact on the operating costs considering data integrity attack using advanced mathematical tools. Future research will also need to take into account additional, possible, relevant constraints,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JESTPE.2020.3015447, IEEE Journal of Emerging and Selected Topics in Power Electronics

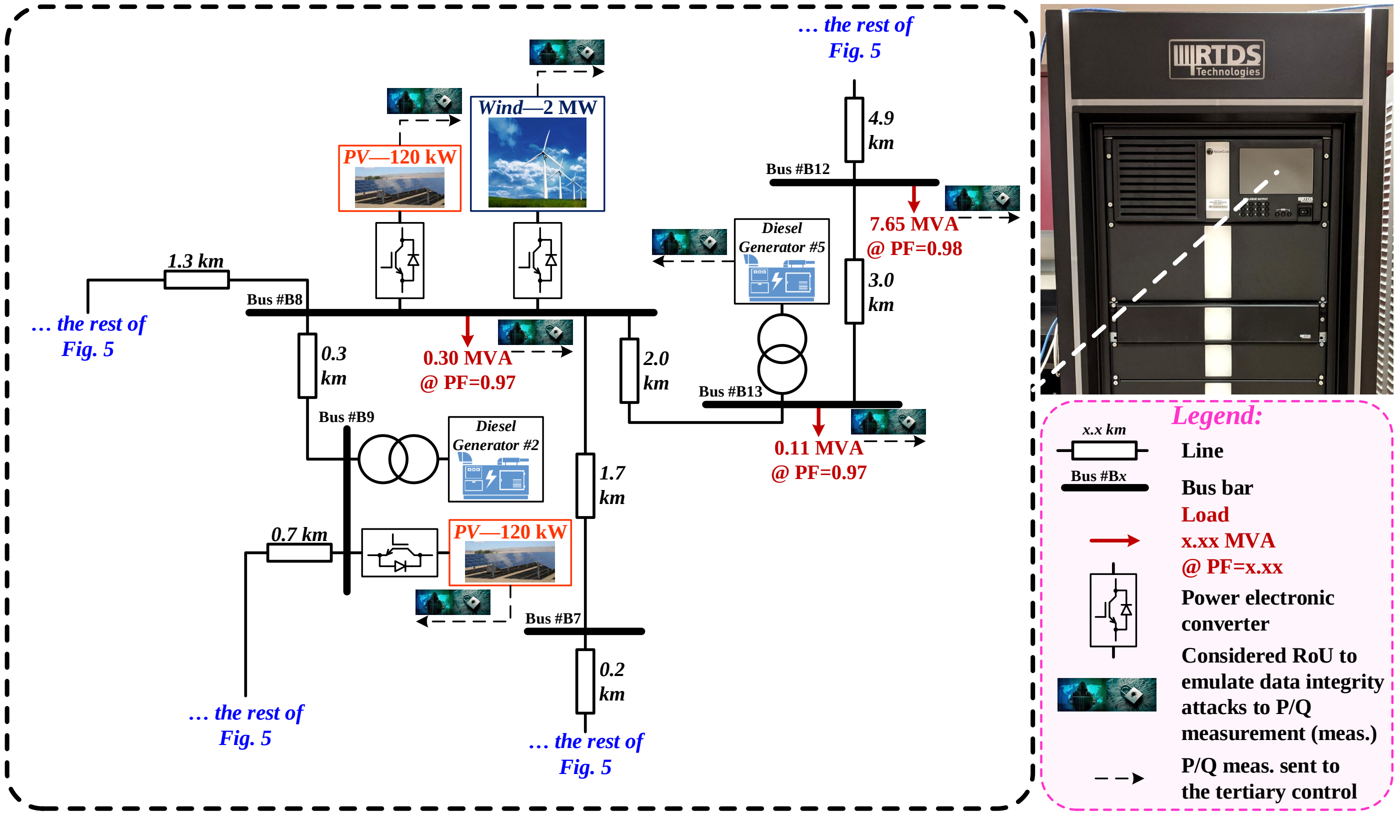

Fig. 16. Demonstration of real-time simulations of the system shown Fig. 5.

TABLE II
DIFFERENT SCENARIOS FOR COMPARATIVE STUDIES OF CT^{2}C IN SUBSUBSECTION III-B1.

Scenario number	δ_{CA} [%]	Gen	Load
S_{1x} Scenarios—*both generating units and load sections*			
S_{11}	200	Yes	Yes
S_{12}	100	Yes	Yes
S_{13}	50	Yes	Yes
S_{14}	10	Yes	Yes
S_{15}	5	Yes	Yes
S_{16}	1	Yes	Yes
S_{2x} Scenarios—*only generating units*			
S_{21}	200	Yes	No
S_{22}	100	Yes	No
S_{23}	50	Yes	No
S_{24}	10	Yes	No
S_{25}	5	Yes	No
S_{26}	1	Yes	No
S_{3x} Scenarios—*only load sections*			
S_{31}	200	No	Yes
S_{32}	100	No	Yes
S_{33}	50	No	Yes
S_{34}	10	No	Yes
S_{35}	5	No	Yes
S_{36}	1	No	Yes

TABLE III
NATURAL NUMBERS ASSIGNED TO DIFFERENT MMG'S ENTITIES IN FIGS. 12 AND 13 IN SUBSUBSECTION III-B2.

Number	Bus#-Entity	Number	Bus#-Entity
1	B1-DG	2	B9-DG
3	B13-DG	4	B5-WT
5	B6-WT	6	B8-WT
7	B3-PV	8	B4-PV
9	B5-PV	10	B6-PV
11	B8-PV	12	B9-PV
13	B10-PV	14	B11-PV
15	B5-BESS	16	B10-BESS
17	B2-Load	18	B3-Load
19	B4-Load	20	B5-Load
21	B6-Load	22	B8-Load
23	B10-Load	24	B11-Load
25	B12-Load	26	B13-Load

TABLE IV
DIFFERENT SCENARIOS FOR COMPARATIVE STUDIES OF CT^{2}C IN SUBSUBSECTION III-B2.

Scenario number	$RoU^{\max}$s[1] [%]	$\frac{OC^{\mathrm{new}}}{OC^{*}} \times 100$ [%]	Gen	Load
S_{4x} Scenarios—*both generating units and load sections*				
S_{41}	4	117	Yes	Yes
S_{42}	3	113	Yes	Yes
S_{43}	2	109	Yes	Yes
S_{44}	1	104	Yes	Yes

[1] For all $K^{\max}_{\mathrm{DG}}$, $K^{\max}_{\mathrm{BESS}}$, $K^{\max}_{\mathrm{PV}}$, $K^{\max}_{\mathrm{WT}}$, and $K^{\max}_{\mathrm{Load}}$

thereby making the optimization process more constrained. To this end, it also mathematically investigates the convex/non-convex issues associated with the "more" constrained optimization problems while data integrity attacks are seen. Last but not least, apart from the elaborated proof of concept, one of the HIL-based techniques is able to involve emulated data

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JESTPE.2020.3015447, IEEE Journal of Emerging and Selected Topics in Power Electronics

integrity attached in the simulation process. Next, more realist, practical implementation of the proposed control via a pilot R & D project is required to be studied and investigated as research activities in the future. Subsection IV-D has outlined the possible, pilot R & D project.

ACKNOWLEDGMENT

The authors would like to thank *RTDS Technologies Inc.* (https://www.rtds.com) for providing partial support to Georgia Southern University. This work has been tested and implemented entirely at Georgia Southern University (Statesboro Campus). They would like to thank the core program of Energy, Power, Control, and Networks (EPCN) in the Division of Electrical, Communications and Cyber Systems (ECCS) from the U.S. National Science Foundation (NSF) has provided the awards.

REFERENCES

[1] Robert H. Lasseter, "Microgrids," in *Proceedings of the IEEE Power Engineering Society Winter Meeting*, Jan. 2002, pp. 305–308.

[2] Federal Energy Regulatory Commission, "Energy Independence and Security Act of 2007, Title XIII—Smart Grid," Online, 2007. [Online]. Available: https://www.govinfo.gov/content/pkg/PLAW-110publ140/pdf/PLAW-110publ140.pdf

[3] M. Davari, W. Gao, and F. Blaabjerg, "A fault-tolerant, passivity-based controller enhanced by the equilibrium-to-equilibrium maneuver capability for the DC-voltage power port VSC in multi-infeed AC/DC modernized grids," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 8, no. 3, pp. 2484–2507, Sep. 2020.

[4] I. D. Woodruff and M. Davari, "An optimization approach based on interior-point methodology for the tertiary control of modernized microgrids," in *Proceedings of the IEEE SoutheastCon 2019*, Apr. 2019, pp. 1–8, DOI: 10.1109/SoutheastCon42311.2019.9020486.

[5] T. Ding, Q. Yang, X. Liu, C. Huang, Y. Yang, M. Wang, and F. Blaabjerg, "Duality-free decomposition based data-driven stochastic security-constrained unit commitment," *IEEE Transactions on Sustainable Energy*, vol. 10, no. 1, pp. 82–93, Jan. 2019.

[6] S. Sahoo, T. Dragičević, and F. Blaabjerg, "Cyber security in control of grid-tied power electronic converters—challenges and vulnerabilities," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, pp. 1–15, 2019, Early Access, DOI: 10.1109/JESTPE.2019.2953480. [Online]. Available: https://ieeexplore.ieee.org/document/8901166

[7] M. Davari, M. P. Aghababa, F. Blaabjerg, and M. Saif, "A modular adaptive robust nonlinear control for resilient integration of vsis into emerging modernized microgrids," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, no. 1–20, 2020, Early Access, DOI: 10.1109/JESTPE.2020.2984231. [Online]. Available: https://ieeexplore.ieee.org/document/9050724

[8] California Energy Commission – Tracking Progress, "Energy Storage," Published Online, Aug. 2018, [Online]. Available: https://www.energy.ca.gov/sites/default/files/2019-12/energy_storage_ada.pdf.

[9] R. Das and V. Madani and A. P. S. Meliopoulos, "Leveraging smart grid technology and using microgrid as a vehicle to benefit DER integration," in *Proceedings of the 2017 IEEE Power & Energy Society InnovativeSmart Grid Technologies Conference (ISGT)*, Apr. 2017, pp. 1–5.

[10] D. Hart and A. Sarkissian, "Deployment of Grid-Scale Batteries in the United States," U.S. Department of Energy, Tech. Rep., Jun. 2016, Prepared for Office of Energy Policy and Systems Analysis, [Online]. Available: https://www.energy.gov/sites/prod/files/2017/01/f34/Deployment

[11] M. Davari, W. Gao, and F. Blaabjerg, "Analysing dynamics and synthesising a robust vector control for the dc-voltage power port based on the modular multilevel converter in multi-infeed AC/DC smart grids," *IET Smart Grid*, vol. 2, no. 4, pp. 645–658, Sep. 2019.

[12] M. Davari and Y. A.-R. I. Mohamed, "Robust multi-objective control of VSC-based DC-voltage power port in hybrid AC/DC multi-terminal micro-grids," *IEEE Transactions on Smart Grid*, vol. 4, no. 3, pp. 1597–1612, Sep. 2013.

[13] J. Shiles, E. Wong, S. Rao, C. Sanden, M. A. Zamani, M. Davari, and F. Katiraei, "Microgrid protection: An overview of protection strategies in North American microgrid projects," in *Proceedings of the IEEE Power & Energy Society General Meeting*, Jul. 2017, pp. 1–5, Published in Feb. 2018.

[14] A. Yazdani and R. Iravani, *Voltage-Sourced Converters in Power Systems: Modeling, Control, and Applications*, 2010, ch. 1, pp. 1–20, Wiley-IEEE Press.

[15] A. Aghazadeh, M. Davari, H. Nafisi, and F. Blaabjerg, "Grid integration of a dual two-level voltage-source inverter considering grid impedance and phase-locked loop," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, 2020, Early Access, DOI: 10.1109/JESTPE.2019.2953522. [Online]. Available: https://ieeexplore.ieee.org/document/8901210

[16] I. U. Nutkani, P. C. Lo, P. Wang, and F. Blaabjerg, "Cost-prioritized droop schemes for autonomous AC microgrids," *IEEE Transactions on Power Electronics*, vol. 30, no. 2, pp. 1109–1119, Feb. 2015.

[17] Z. Zhao and G. Chen, "An overview of cyber security for smart grid," in *Proceedings of the IEEE 27th International Symposium on Industrial Electronics (ISIE)*. IEEE, 2018, pp. 1127–1131.

[18] A. O. Otuoze, M. W. Mustafa, and R. M. Larik, "Smart grids security challenges: Classification by sources of threats," *Journal of Electrical Systems and Information Technology*, vol. 5, no. 3, pp. 468–483, Dec. 2018, ScienceDirect.

[19] L. Langer, P. Smith, and M. Hutle, "Smart grid cybersecurity risk assessment," in *Proceedings of the International Symposium on Smart Electric Distribution Systems and Technologies (EDST)*. IEEE, 2015, pp. 475–482.

[20] P. Kaster and P. K. Sen, "Power grid cyber security: Challenges and impacts," in *Proceedings of 2014 North American Power Symposium (NAPS)*. IEEE, 2014, pp. 1–6.

[21] G. C. Wilshusen and D. C. Trimble, "CYBERSECURITY challenges in securing the electricity grid," Online, Feb. 2012, Testimony Before the Senate Committee on Energy and Natural Resources, Statement of Gregory C. Wilshusen GAO-12-507T.

[22] J. E. Dagle, "Cyber security of the electric power grid," in *Proceedings of the IEEE/PES Power Systems Conference and Exposition*. IEEE, 2009, pp. 1–2.

[23] IBM Security, "Cybersecurity for Energy, Environment and Utilities," [Online]. Available: https://www.ibm.com/security/industry/energy-environment-utilities.

[24] ICF International, "Electric grid security and resilience—establishing a baseline for adversarial threats," Online, Tech. Rep., Jun. 2016, report for the Agencies of the United States and Canadian Governments, [Online].

[25] Z. Cheng, J. Duan, and M.-Y. Chow, "To centralize or to distribute: That is the question," *IEEE Industrial Electronics Magazine*, vol. 12, no. 1, pp. 6–24, Mar. 2018.

[26] P. Martí, M. Velasco, E. X. Martín, L. G. de Vicuña, J. Miret, and M. Castilla, "Performance evaluation of secondary control policies with respect to digital communications properties in inverter-based islanded microgrids," *IEEE Transactions on Smart Grid*, vol. 9, no. 3, pp. 2192–2202, May 2018.

[27] R. V. A. Neves, R. Q. Machado, V. A. Oliveira, X. Wang, and F. Blaabjerg, "Multitask fuzzy secondary controller for AC microgrid operating in stand-alone and grid-tied mode," *IEEE Transactions on Smart Grid*, vol. PP, no. 99, pp. 1–9, 2019, early Access, [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8584132.

[28] T. Morstyn, A. V. Savkin, B. Hredzak, and H. D. Tuan, "Scalable energy management for low voltage microgrids using multi-agent storage system aggregation," *IEEE Transactions on Power Systems*, vol. 33, no. 2, pp. 1614–1623, Mar. 2018.

[29] A. Arefi and F. Shahnia, "Tertiary controller-based optimal voltage and frequency management technique for multi-microgrid systems of large remote towns," *IEEE Transactions on Smart Grid*, vol. 9, no. 6, pp. 5962–5974, Nov. 2018.

[30] J. Duan, Z. Yi, D. Shi, C. Lin, X. Lu, and Z. Wang, "Reinforcement-learning-based optimal control for hybrid energy storage systems in hybrid AC/DC microgrids," *IEEE Transactions on Industrial Informatics*, vol. PP, no. 99, pp. 1–10, 2019, early Access, [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8630643.

[31] X. Liu, C. Qian, W. G. Hatcher, H. Xu, W. Liao, and W. Yu, "Secure internet of things (IoT)-based smart-world critical infrastructures: survey, case study and research opportunities," *IEEE Access*, vol. 7, pp. 79 523–79 544, Jun. 2019.

[32] R. Deng, G. Xiao, R. Lu, H. Liang, and A. V. Vasilakos, "False data injection on state estimation in power systems—Attacks, impacts, and

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JESTPE.2020.3015447, IEEE Journal of Emerging and Selected Topics in Power Electronics

defense: A survey," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 2, pp. 411–423, Apr. 2017.
[33] Q. Yang, J. Yang, W. Yu, D. An, N. Zhang, and W. Zhao, "On false data-injection attacks against power system state estimation: Modeling and countermeasures," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 3, pp. 717–729, Mar. 2014.
[34] Q. Yang, D. Li, W. Yu, Y. Liu, D. An, X. Yang, and J. Lin, "Toward data integrity attacks against optimal power flow in smartgrid," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1726–1738, Oct. 2017.
[35] C. Zhao, J. He, and P. Cheng, and J. Chen, "Analysis of consensus-based distributed economic dispatch under stealthy attacks," *IEEE Transactions on Industrial Electronics*, vol. 64, no. 6, pp. 5107–5117, Jun. 2017.
[36] T. McBride, M. Ekstrom, L. Lusty, J. Sexton, and A. Townsend, "Data integrity: Recovering from ransomware and other destructive events," Online, Sep. 2017, NIST Special Publication 1800-11. [Online]. Available: https://www.nccoe.nist.gov/sites/default/files/library/sp1800/di-nist-sp1800-11-draft.pdf
[37] Y. Feng, S. Huang, Q. A. Chen, H. X. Liu, and Z. M. Mao, "Vulnerability of traffic control system under cyberattacks with falsified data," *Transportation Research Record: Journal of the Transportation Research Board*, vol. 2672, no. 1, pp. 1–11, Mar. 2018.
[38] Bipartisan Policy Center Electric Grid Cybersecurity Initiative Participants, "Cybersecurity and the North American Electric Grid: New Policy Approaches to Address an Evolving Threat," Published Online, Feb. 2014, A Report from the Co-chairs of the Bipartisan Policy Center's Electric Grid Cybersecurity Initiative, Energy & Infrastructure Program and National Security Program. [Online]. Available: https://bipartisanpolicy.org/wp-content/uploads/2019/03/Cybersecurity-Electric-Grid-BPC.pdf
[39] Mission Support Center, "Cyber Threat and Vulnerability Analysisof the U.S. Electric Sector," Idaho National Laboratory, resreport INL/EXT-16-40692, Aug. 2016, Mission Support Center Analysis Report, Published Online. [Online]. Available: https://www.energy.gov/sites/prod/files/2017/01/f34/Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector.pdf
[40] Y. Ben-Haim, *Information-gap Decision Theory: Decisions Under Severe Uncertainty*, ser. Academic Press Series on Decision and Risk. Academic Press, 2001. [Online]. Available: https://books.google.com/books?id=8CnvAAAAMAAJ
[41] M.-A. Nasr, E. Nasr-Azadani, and H. Nafisi, S. H. Hosseinian, and P. Siano, "Assessing the effectiveness of weighted information gap decision theory integrated with energy management systems for isolated microgrids," *IEEE Transactions on Industrial Informatics*, pp. 1–12, 2019, Early Access, DOI: 10.1109/TII.2019.2954706. [Online]. Available: https://ieeexplore.ieee.org/document/8907393
[42] "General Algebraic Modeling System (GAMS) Release 24.2.1," Washington, DC, USA, GAMS Development Corporation, 2013. [Online]. Available: http://www.gams.com/
[43] *GAMS - A User's Guide, GAMS Release 24.2.1*, GAMS Development Corporation, Washington, DC, USA, 2013. [Online]. Available: http://www.gams.com/dd/docs/bigdocs/GAMSUsersGuide.pdf
[44] RTDS Technologies Inc., "NovaCor a new generation of simulation hardware for the RTDS simulator," Aug. 2018, More Information Can Be Found on https://legacy.rtds.com/novacor/. [Online]. Available: https://www.rtds.com/wp-content/uploads/2019/08/NovaCor.pdf

Masoud Davari (S'08–M'17–SM'19) was born in Isfahan, Iran, on September 14, 1985. He received the B.Sc. degree (with Distinction) in electrical engineering-power from the Isfahan University of Technology, Isfahan, Iran, in September 2007, the M.Sc. degree (with Distinction) in electrical engineering-power from the Amirkabir University of Technology (Tehran Polytechnic), Tehran, Iran, in January 2010, and the Ph.D. degree in electrical engineering-energy systems from the University of Alberta, Edmonton, AB, Canada, in January 2016.

He was with Iran's Grid Secure Operation Research Center and Iran's Electric Power Research Institute (EPRI) in Tehran, Iran, from January 2010 to December 2011. From April 2015 to June 2017, he has been collaborating with Quanta-Technology Company, Markham, ON, Canada, in the field of the dynamic interaction of renewable energy systems with smart grids as well as control, protection, and automation of microgrids as a Senior R & D Specialist and Senior Consultant. In July 2017, he joined the Department of Electrical and Computer Engineering in Allen E. Paulson College of Engineering and Computing at Georgia Southern University, Statesboro, GA, USA, as a tenure-track Assistant Professor. He has developed and implemented several experimental test rigs for both research universities and the industry. He has also authored several IEEE Transactions and Journals. He is also the invited reviewer of several of the IEEE TRANSACTIONS and Journals, IET journals, Energies Journal, and various IEEE conferences, as well as the invited speaker at different universities and in diverse societies. He was awarded the Best Reviewer of the IEEE TRANSACTIONS ON POWER SYSTEMS in 2018. His research interests include the dynamics, controls, and protections of different types of power electronic converters, which are utilized in the hybrid ac/dc smart grids, and hardware-in-the-loop (HIL) testing of modernized power systems.

Dr. Davari serves as an active member and a chapter lead (for Chapter 3) in the IEEE WG P2004, a newly established IEEE working group on the HIL simulation for IEEE Standards Association, from June 2017 until now. He is an invited member of the Golden Key International Honour Society. He served as the chair of the Literature Review Subgroup of DC@home Standards for the IEEE Standards Association from April 2014 to October 2015.

Hamed Nafisi was born in Tehran, Iran. He received the B.Sc., M.Sc., and Ph.D. degrees in electrical engineering from the Amirkabir University of Technology, Tehran, Iran, in 2006, 2008, and 2014, respectively. He is currently an Assistant Professor with the Department of Electrical Engineering, Amirkabir University of Technology. His current research interests include smart grids, power system protection, and power electronics application in power systems.

Mohamad-Amin Nasr received the M.Sc. (with Distinction) degree in electrical engineering from the Iranian Center of Excellence in Power Systems, Amirkabir University of Technology (Tehran Polytechnic), Tehran, Iran, in October 2019.

He has been a Member of Iranian National Elites since 2018. His current research interests include advanced optimization techniques and the operation, control, and protection of power systems and microgrids in the presence of highly variable renewable energy sources.

Frede Blaabjerg (S'86–M'88–SM'97–F'03) received the Ph.D. degree in electrical engineering from Aalborg University, Aalborg, Denmark, in 1995, and the honoris causa degree from the University Politehnica Timisoara the University Politehnica Timisoara (UPT), Timisoara, Romania, in 2017, and Tallinn Technical University (TTU), Tallinn, Estonia in 2018.

He was with ABB-Scandia, Randers, Denmark, from 1987 to 1988. He became an Assistant Professor with the Department of Energy Technology, Aalborg University, in 1992, an Associate Professor in 1996, and a Full Professor of power electronics and drives in 1998, where he has been a Villum Investigator since 2017. He has authored or coauthored more than 600 journal articles in different fields of power electronics and its applications, coauthored four monographs, and edited ten books in power electronics and its applications. His current research interests include power electronics and its applications, such as in wind turbines, photovoltaic systems, reliability, harmonics, and adjustable speed drives.

Dr. Blaabjerg received the 31 IEEE Prize Paper Awards, the IEEE PELS Distinguished Service Award in 2009, the EPE-PEMC Council Award in 2010, the IEEE William E. Newell Power Electronics Award 2014, and the Villum Kann Rasmussen Research Award 2014. He was a recipient of the Global Energy Award for a significant contribution to the development of technologies that provide new energy development opportunities in 2019. He was a recipient of the IEEE Edison Medal in 2020. He is the President of the IEEE Power Electronics Society for 2019–2020 and the Vice President of the Danish Academy of Technical Sciences. He was the Editor-in-Chief of the IEEE IEEE TRANSACTIONS ON POWER ELECTRONICS from 2006 to 2012. He was a Distinguished Lecturer of the IEEE Power Electronics Society from 2005 to 2007 and the IEEE Industry Applications Society from 2010 to 2011 and 2017 to 2018. He was nominated by Thomson Reuters to be included in the 250 most cited researchers in engineering in the world in 2014–2018.